

Aayush Shah

19BCE245

24 November 2020

Truth table

Square root under modulo p

- Is square root under modulo p is exists or not ? - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	0
1:	0	0	0	0	0	1	0
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	0
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	0
7:	0	0	0	1	1	1	1
8:	0	0	1	0	0	0	0
9:	0	0	1	0	0	1	0
10:	0	0	1	0	1	0	0
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	0
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	0
15:	0	0	1	1	1	1	0
16:	0	1	0	0	0	0	0
17:	0	1	0	0	0	1	1
18:	0	1	0	0	1	0	0
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	0
21:	0	1	0	1	0	1	0
22:	0	1	0	1	1	0	0
23:	0	1	0	1	1	1	1
24:	0	1	1	0	0	0	0
25:	0	1	1	0	0	1	0
26:	0	1	1	0	1	0	0
27:	0	1	1	0	1	1	0
28:	0	1	1	1	0	0	0
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	0
31:	0	1	1	1	1	1	1

32:	1	0	0	0	0	0	0
33:	1	0	0	0	0	1	0
34:	1	0	0	0	1	0	0
35:	1	0	0	0	1	1	0
36:	1	0	0	1	0	0	0
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	0
39:	1	0	0	1	1	1	0
40:	1	0	1	0	0	0	0
41:	1	0	1	0	0	1	0
42:	1	0	1	0	1	0	1
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	0
45:	1	0	1	1	0	1	0
46:	1	0	1	1	1	0	0
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	0
49:	1	1	0	0	0	1	0
50:	1	1	0	0	1	0	0
51:	1	1	0	0	1	1	0
52:	1	1	0	1	0	0	0
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	0
55:	1	1	0	1	1	1	0
56:	1	1	1	0	0	0	0
57:	1	1	1	0	0	1	0
58:	1	1	1	0	1	0	0
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	0
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	0
63:	1	1	1	1	1	1	0

Minimal boolean expression:

$$y = (\bar{x}_5 \bar{x}_3 x_2 x_1 x_0) + (\bar{x}_5 x_4 \bar{x}_3 \bar{x}_2 \bar{x}_1 x_0) + (\bar{x}_5 x_4 x_2 x_1 x_0) + (x_5 \bar{x}_4 x_3 \bar{x}_2 x_1 \bar{x}_0)$$

• Digit 1 - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	×
1:	0	0	0	0	0	1	×
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	×
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	×
7:	0	0	0	1	1	1	0
8:	0	0	1	0	0	0	×
9:	0	0	1	0	0	1	×
10:	0	0	1	0	1	0	×
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	×
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	×
15:	0	0	1	1	1	1	×
16:	0	1	0	0	0	0	×
17:	0	1	0	0	0	1	0
18:	0	1	0	0	1	0	×
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	×
21:	0	1	0	1	0	1	×
22:	0	1	0	1	1	0	×
23:	0	1	0	1	1	1	0
24:	0	1	1	0	0	0	×
25:	0	1	1	0	0	1	×
26:	0	1	1	0	1	0	×
27:	0	1	1	0	1	1	×
28:	0	1	1	1	0	0	×
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	×
31:	0	1	1	1	1	1	0
32:	1	0	0	0	0	0	×
33:	1	0	0	0	0	1	×
34:	1	0	0	0	1	0	×
35:	1	0	0	0	1	1	×
36:	1	0	0	1	0	0	×
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	×

Minimal boolean expression:

$$y = (x_5 \bar{x}_4 x_3 \bar{x}_1)$$

39:	1	0	0	1	1	1	×
40:	1	0	1	0	0	0	×
41:	1	0	1	0	0	1	1
42:	1	0	1	0	1	0	×
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	×
45:	1	0	1	1	0	1	×
46:	1	0	1	1	1	0	×
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	×
49:	1	1	0	0	0	1	×
50:	1	1	0	0	1	0	×
51:	1	1	0	0	1	1	×
52:	1	1	0	1	0	0	×
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	×
55:	1	1	0	1	1	1	×
56:	1	1	1	0	0	0	×
57:	1	1	1	0	0	1	×
58:	1	1	1	0	1	0	×
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	×
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	×
63:	1	1	1	1	1	1	×

• Digit 2 - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	×
1:	0	0	0	0	0	1	×
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	×
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	×
7:	0	0	0	1	1	1	0
8:	0	0	1	0	0	0	×
9:	0	0	1	0	0	1	×
10:	0	0	1	0	1	0	×
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	×
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	×
15:	0	0	1	1	1	1	×
16:	0	1	0	0	0	0	×
17:	0	1	0	0	0	1	1
18:	0	1	0	0	1	0	×
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	×
21:	0	1	0	1	0	1	×
22:	0	1	0	1	1	0	×
23:	0	1	0	1	1	1	1
24:	0	1	1	0	0	0	×
25:	0	1	1	0	0	1	×
26:	0	1	1	0	1	0	×
27:	0	1	1	0	1	1	×
28:	0	1	1	1	0	0	×
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	×
31:	0	1	1	1	1	1	0
32:	1	0	0	0	0	0	×
33:	1	0	0	0	0	1	×
34:	1	0	0	0	1	0	×
35:	1	0	0	0	1	1	×
36:	1	0	0	1	0	0	×
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	×

Minimal boolean expression:

$$y = (\bar{x}_5 x_4 \bar{x}_3 \bar{x}_1) \vee (\bar{x}_5 x_4 \bar{x}_3 x_2)$$

39:	1	0	0	1	1	1	×
40:	1	0	1	0	0	0	×
41:	1	0	1	0	0	1	0
42:	1	0	1	0	1	0	×
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	×
45:	1	0	1	1	0	1	×
46:	1	0	1	1	1	0	×
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	×
49:	1	1	0	0	0	1	×
50:	1	1	0	0	1	0	×
51:	1	1	0	0	1	1	×
52:	1	1	0	1	0	0	×
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	×
55:	1	1	0	1	1	1	×
56:	1	1	1	0	0	0	×
57:	1	1	1	0	0	1	×
58:	1	1	1	0	1	0	×
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	×
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	×
63:	1	1	1	1	1	1	×

•Digit 3 - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	×
1:	0	0	0	0	0	1	×
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	×
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	×
7:	0	0	0	1	1	1	1
8:	0	0	1	0	0	0	×
9:	0	0	1	0	0	1	×
10:	0	0	1	0	1	0	×
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	×
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	×
15:	0	0	1	1	1	1	×
16:	0	1	0	0	0	0	×
17:	0	1	0	0	0	1	1
18:	0	1	0	0	1	0	×
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	×
21:	0	1	0	1	0	1	×
22:	0	1	0	1	1	0	×
23:	0	1	0	1	1	1	0
24:	0	1	1	0	0	0	×
25:	0	1	1	0	0	1	×
26:	0	1	1	0	1	0	×
27:	0	1	1	0	1	1	×
28:	0	1	1	1	0	0	×
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	×
31:	0	1	1	1	1	1	0
32:	1	0	0	0	0	0	×
33:	1	0	0	0	0	1	×
34:	1	0	0	0	1	0	×
35:	1	0	0	0	1	1	×
36:	1	0	0	1	0	0	×
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	×

Minimal boolean expression:

$$y = (\bar{x}_5 \bar{x}_4 x_2 x_1) \vee (\bar{x}_5 x_4 \bar{x}_3 \bar{x}_1)$$

39:	1	0	0	1	1	1	×
40:	1	0	1	0	0	0	×
41:	1	0	1	0	0	1	0
42:	1	0	1	0	1	0	×
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	×
45:	1	0	1	1	0	1	×
46:	1	0	1	1	1	0	×
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	×
49:	1	1	0	0	0	1	×
50:	1	1	0	0	1	0	×
51:	1	1	0	0	1	1	×
52:	1	1	0	1	0	0	×
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	×
55:	1	1	0	1	1	1	×
56:	1	1	1	0	0	0	×
57:	1	1	1	0	0	1	×
58:	1	1	1	0	1	0	×
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	×
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	×
63:	1	1	1	1	1	1	×

• Digit 4 - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	×
1:	0	0	0	0	0	1	×
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	×
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	×
7:	0	0	0	1	1	1	0
8:	0	0	1	0	0	0	×
9:	0	0	1	0	0	1	×
10:	0	0	1	0	1	0	×
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	×
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	×
15:	0	0	1	1	1	1	×
16:	0	1	0	0	0	0	×
17:	0	1	0	0	0	1	0
18:	0	1	0	0	1	0	×
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	×
21:	0	1	0	1	0	1	×
22:	0	1	0	1	1	0	×
23:	0	1	0	1	1	1	0
24:	0	1	1	0	0	0	×
25:	0	1	1	0	0	1	×
26:	0	1	1	0	1	0	×
27:	0	1	1	0	1	1	×
28:	0	1	1	1	0	0	×
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	×
31:	0	1	1	1	1	1	1
32:	1	0	0	0	0	0	×
33:	1	0	0	0	0	1	×
34:	1	0	0	0	1	0	×
35:	1	0	0	0	1	1	×
36:	1	0	0	1	0	0	×
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	×

Minimal boolean expression:

$$y = (\bar{x}_5 x_3 x_2 x_1)$$

39:	1	0	0	1	1	1	×
40:	1	0	1	0	0	0	×
41:	1	0	1	0	0	1	0
42:	1	0	1	0	1	0	×
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	×
45:	1	0	1	1	0	1	×
46:	1	0	1	1	1	0	×
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	×
49:	1	1	0	0	0	1	×
50:	1	1	0	0	1	0	×
51:	1	1	0	0	1	1	×
52:	1	1	0	1	0	0	×
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	×
55:	1	1	0	1	1	1	×
56:	1	1	1	0	0	0	×
57:	1	1	1	0	0	1	×
58:	1	1	1	0	1	0	×
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	×
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	×
63:	1	1	1	1	1	1	×

• Digit 5 - TRUTH-TABLE

	x_5	x_4	x_3	x_2	x_1	x_0	y
0:	0	0	0	0	0	0	×
1:	0	0	0	0	0	1	×
2:	0	0	0	0	1	0	0
3:	0	0	0	0	1	1	0
4:	0	0	0	1	0	0	×
5:	0	0	0	1	0	1	0
6:	0	0	0	1	1	0	×
7:	0	0	0	1	1	1	0
8:	0	0	1	0	0	0	×
9:	0	0	1	0	0	1	×
10:	0	0	1	0	1	0	×
11:	0	0	1	0	1	1	0
12:	0	0	1	1	0	0	×
13:	0	0	1	1	0	1	0
14:	0	0	1	1	1	0	×
15:	0	0	1	1	1	1	×
16:	0	1	0	0	0	0	×
17:	0	1	0	0	0	1	0
18:	0	1	0	0	1	0	×
19:	0	1	0	0	1	1	0
20:	0	1	0	1	0	0	×
21:	0	1	0	1	0	1	×
22:	0	1	0	1	1	0	×
23:	0	1	0	1	1	1	1
24:	0	1	1	0	0	0	×
25:	0	1	1	0	0	1	×
26:	0	1	1	0	1	0	×
27:	0	1	1	0	1	1	×
28:	0	1	1	1	0	0	×
29:	0	1	1	1	0	1	0
30:	0	1	1	1	1	0	×
31:	0	1	1	1	1	1	0
32:	1	0	0	0	0	0	×
33:	1	0	0	0	0	1	×
34:	1	0	0	0	1	0	×
35:	1	0	0	0	1	1	×
36:	1	0	0	1	0	0	×
37:	1	0	0	1	0	1	0
38:	1	0	0	1	1	0	×

Minimal boolean expression:

$$y = (\bar{x}_5 x_4 \bar{x}_3 x_2) \vee (x_5 \bar{x}_4 x_3 \bar{x}_1)$$

39:	1	0	0	1	1	1	×
40:	1	0	1	0	0	0	×
41:	1	0	1	0	0	1	1
42:	1	0	1	0	1	0	×
43:	1	0	1	0	1	1	0
44:	1	0	1	1	0	0	×
45:	1	0	1	1	0	1	×
46:	1	0	1	1	1	0	×
47:	1	0	1	1	1	1	0
48:	1	1	0	0	0	0	×
49:	1	1	0	0	0	1	×
50:	1	1	0	0	1	0	×
51:	1	1	0	0	1	1	×
52:	1	1	0	1	0	0	×
53:	1	1	0	1	0	1	0
54:	1	1	0	1	1	0	×
55:	1	1	0	1	1	1	×
56:	1	1	1	0	0	0	×
57:	1	1	1	0	0	1	×
58:	1	1	1	0	1	0	×
59:	1	1	1	0	1	1	0
60:	1	1	1	1	0	0	×
61:	1	1	1	1	0	1	0
62:	1	1	1	1	1	0	×
63:	1	1	1	1	1	1	×

Snaps of circuit

