

Table of $x^{**}y \text{ mod } 29$

x =	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
y = 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
2	4	9	16	25	7	20	6	23	13	5	28	24	22	22	24	28	5	13	23	6	20	7	25	16	9	4	1
3	8	27	6	9	13	24	19	4	14	26	17	22	18	11	7	12	3	15	25	10	5	16	20	23	2	21	28
4	16	23	24	16	20	23	7	7	24	25	1	25	20	20	25	1	25	24	7	7	23	20	16	24	23	16	1
5	3	11	9	22	4	16	27	5	8	14	12	6	19	10	23	17	15	21	24	2	13	25	7	20	18	26	28
6	6	4	7	23	24	25	13	16	22	9	28	20	5	5	20	28	9	22	16	13	25	24	23	7	4	6	1
7	12	12	28	28	28	1	17	28	17	12	17	28	12	17	1	12	17	12	1	12	28	1	1	1	17	17	28
8	24	7	25	24	23	7	20	20	25	16	1	16	23	23	16	1	16	25	20	20	7	23	24	25	7	24	1
9	19	21	13	4	22	20	15	6	18	2	12	5	3	26	24	17	27	11	23	14	9	7	25	16	8	10	28
10	9	5	23	20	16	24	4	25	6	22	28	7	13	13	7	28	22	6	25	4	24	16	20	23	5	9	1
11	18	15	5	13	9	23	3	22	2	10	17	4	8	21	25	12	19	27	7	26	6	20	16	24	14	11	28
12	7	16	20	7	25	16	24	24	20	23	1	23	25	25	23	1	23	20	24	24	16	25	7	20	16	7	1
13	14	19	22	6	5	25	18	13	26	21	12	9	2	27	20	17	8	3	16	11	4	24	23	7	10	15	28
14	28	28	1	1	1	1	28	1	28	28	28	1	28	28	1	28	28	28	1	28	1	1	1	1	28	28	1
15	27	26	4	5	6	7	21	9	19	18	17	13	15	14	16	12	11	10	20	8	22	23	24	25	3	2	28
16	25	20	16	25	7	20	23	23	16	24	1	24	7	7	24	1	24	16	23	23	20	7	25	16	20	25	1
17	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14	25	19	5	16	20	23	27	8	28
18	13	6	24	16	20	23	22	7	5	4	28	25	9	9	25	28	4	5	7	22	23	20	16	24	6	13	1
19	26	18	9	22	4	16	2	5	21	15	17	6	10	19	23	12	14	8	24	27	13	25	7	20	11	3	28
20	23	25	7	23	24	25	16	16	7	20	1	20	24	24	20	1	20	7	16	16	25	24	23	7	25	23	1
21	17	17	28	28	28	1	12	28	12	17	12	28	17	12	1	17	12	17	1	17	28	1	1	1	12	12	28
22	5	22	25	24	23	7	9	20	4	13	28	16	6	6	16	28	13	4	20	9	7	23	24	25	22	5	1
23	10	8	13	4	22	20	14	6	11	27	17	5	26	3	24	12	2	18	23	15	9	7	25	16	21	19	28
24	20	24	23	20	16	24	25	25	23	7	1	7	16	16	7	1	7	23	25	25	24	16	20	23	24	20	1
25	11	14	5	13	9	23	26	22	27	19	12	4	21	8	25	17	10	2	7	3	6	20	16	24	15	18	28
26	22	13	20	7	25	16	5	24	9	6	28	23	4	4	23	28	6	9	24	5	16	25	7	20	13	22	1
27	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28
28	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	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

For example, let's say you want $14^{**}20 \text{ mod } 29$.
 The answer is the cell at column 14 and row 20, which equals 24.

Note that columns 1 and 29 are omitted. They would not be very interesting.

In real life, p would be a prime much larger than 29. It could have hundreds of digits.
 If $p = 29$, it would be too easy for Eve to determine a or b . She could just look down the appropriate column and find the answer.
 For example, Eve might want to solve $15^{**}a \text{ mod } 29 = 12$, based on info sent from Alice.
 To solve, we look down column 15. Which row has a cell value result of 12? We see that $a = 21$.

Instead, p should be so large that it would be impractical to produce a table like this, and trying all the possibilities down one of the columns would take an inordinate amount of time.

Table of $x^{**}y \pmod{31}$

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

Table of $x^{**}y \pmod{37}$

x =	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		
y =	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	
	2	4	8	16	32	27	17	34	12	9	26	10	33	21	11	3	34	30	28	28	30	34	3	11	21	33	10	26	7	27	12	36	25	16	9	4	1
	3	8	27	27	14	31	10	31	26	1	36	26	14	6	8	26	29	23	14	8	11	29	31	23	11	1	36	11	6	27	6	23	10	10	29	36	
	4	16	7	34	33	1	33	26	12	10	26	16	34	10	9	9	12	7	7	12	9	9	10	34	16	26	10	12	26	33	1	33	34	7	16	1	
	5	32	21	25	17	6	9	23	34	26	27	7	35	29	24	33	19	15	22	18	4	13	8	2	30	10	11	3	14	28	31	20	12	16	5	36	
	6	27	26	26	11	36	26	36	10	1	1	10	11	36	27	10	27	11	11	27	10	27	36	11	10	1	1	10	36	26	36	11	26	26	27	1	
	7	17	4	30	18	31	34	29	16	10	11	9	32	23	35	12	15	13	24	22	25	2	14	5	28	26	27	21	8	3	6	19	7	33	20	36	
	8	34	12	9	16	1	16	10	33	26	10	34	9	26	7	7	33	12	12	33	7	7	26	9	34	10	26	33	10	16	1	16	9	12	34	1	
	9	31	36	36	6	6	1	6	1	1	36	1	6	31	31	1	6	31	6	31	36	6	6	31	36	1	36	36	31	36	31	31	1	1	6	36	
	10	25	34	33	30	36	7	11	9	10	26	12	4	27	21	16	28	3	3	28	16	21	27	4	12	26	10	9	11	7	36	30	33	34	25	1	
	11	13	28	21	2	31	12	14	7	26	27	33	15	8	19	34	32	17	20	5	3	18	29	22	4	10	11	30	23	25	6	35	16	9	24	36	
	12	26	10	10	10	1	10	1	26	1	1	26	10	1	26	26	26	10	10	26	26	26	1	10	26	1	1	26	1	10	1	10	10	10	10	26	1
	13	15	30	3	13	6	33	8	12	10	11	16	19	14	20	9	35	32	5	2	28	17	23	18	21	26	27	25	29	4	31	24	34	7	22	36	
	14	30	16	12	28	36	9	27	34	26	10	7	25	11	4	33	3	21	21	3	33	4	11	25	7	10	26	34	27	9	36	28	12	16	30	1	
	15	23	11	11	29	31	26	31	10	1	36	10	29	6	23	10	14	8	29	23	27	14	31	8	27	1	36	27	6	11	6	8	26	26	14	36	
	16	9	33	7	34	1	34	26	16	10	26	9	7	10	12	12	16	33	33	16	12	12	10	7	9	26	10	16	26	34	1	34	7	33	9	1	
	17	18	25	28	22	6	16	23	33	26	27	34	17	29	32	7	13	2	35	24	30	5	8	20	3	10	11	4	14	21	31	15	9	12	19	36	
	18	36	1	1	36	36	1	36	1	1	1	1	36	36	36	1	36	36	36	36	1	36	36	36	1	1	1	1	36	1	36	36	1	1	36	1	
	19	35	3	4	32	31	7	29	9	10	11	12	24	23	22	16	20	19	18	17	21	15	14	13	25	26	27	28	8	30	6	5	33	34	2	36	
	20	33	9	16	12	1	12	10	7	26	10	33	16	26	34	34	7	9	9	7	34	34	26	16	33	10	26	7	10	12	1	12	16	9	33	1	
	21	29	27	27	23	6	10	6	26	1	36	26	23	31	29	26	8	14	23	29	11	8	6	14	11	1	36	11	31	27	31	14	10	10	8	36	
	22	21	7	34	4	36	33	11	12	10	26	16	3	27	28	9	25	30	30	25	9	28	27	3	16	26	10	12	11	33	36	4	34	7	21	1	
	23	5	21	25	20	31	9	14	34	26	27	7	2	8	13	33	18	22	15	19	4	24	29	35	30	10	11	3	23	28	6	17	12	16	32	36	
	24	10	26	26	26	1	26	1	10	1	1	10	26	1	10	10	10	26	26	10	10	10	1	26	10	1	1	10	1	26	1	26	26	26	10	1	
	25	20	4	30	19	6	34	8	16	10	11	9	5	14	2	12	22	24	13	15	25	35	23	32	28	26	27	21	29	3	31	18	7	33	17	36	
	26	3	12	9	21	36	16	27	33	26	10	34	28	11	30	7	4	25	25	4	7	30	11	28	34	10	26	33	27	16	36	21	9	12	3	1	
	27	6	36	36	31	31	1	31	1	1	36	1	31	6	6	1	31	6	31	6	36	31	31	6	36	1	36	36	6	36	6	6	1	1	31	36	
	28	12	34	33	7	1	7	26	9	10	26	12	33	10	16	16	9	34	34	9	16	16	10	33	12	26	10	9	26	7	1	7	33	34	12	1	
	29	24	28	21	35	6	12	23	7	26	27	33	22	29	18	34	5	20	17	32	3	19	8	15	4	10	11	30	14	25	31	2	16	9	13	36	
	30	11	10	10	27	36	10	36	26	1	1	26	27	36	11	26	11	27	27	11	26	11	36	27	26	1	1	26	36	10	36	27	10	10	11	1	
	31	22	30	3	24	31	33	29	12	10	11	16	18	23	17	9	2	5	32	35	28	20	14	19	21	26	27	25	8	4	6	13	34	7	15	36	
	32	7	16	12	9	1	9	10	34	26	10	7	12	26	33	33	34	16	16	34	33	33	26	12	7	10	26	34	10	9	1	9	12	16	7	1	
	33	14	11	11	8	6	26	6	10	1	36	10	8	31	14	10	23	29	8	14	27	23	6	29	27	1	36	27	31	11	31	29	26	26	23	36	
	34	28	33	7	3	36	34	11	16	10	26	9	30	27	25	12	21	4	4	21	12	25	27	30	9	26	10	16	11	34	36	3	7	33	28	1	
	35	19	25	28	15	31	16	14	33	26	27	34	20	8	5	7	24	35	2	13	30	32	29	17	3	10	11	4	23	21	6	22	9	12	18	36	
	36	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	37	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	