

$$i2^k \pmod n$$

Ian McLoughlin

September 23, 2016

**2**

---

0	0
1	0

---

**3**

---

0	0
1	2
2	1

---

**4**

---

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

---

**5**

---

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

---

**6**

---

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

---

**7**

---

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

---

**8**

---

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

---

**9**

---

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

---

## 10

---

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

---

## 11

---

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

---

## 12

---

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

---

## 13

---

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

---

## 14

---

0	0	0	0
1	2	4	8
2	4	8	2
3	6	12	10
4	8	2	4
5	10	6	12
6	12	10	6
7	0	0	0
8	2	4	8
9	4	8	2
10	6	12	10
11	8	2	4
12	10	6	12
13	12	10	6

---

## 15

---

0	0	0	0
1	2	4	8
2	4	8	1
3	6	12	9
4	8	1	2
5	10	5	10
6	12	9	3
7	14	13	11
8	1	2	4
9	3	6	12
10	5	10	5
11	7	14	13
12	9	3	6
13	11	7	14
14	13	11	7

---

## 16

---

0	0	0	0	0
1	2	4	8	0
2	4	8	0	0
3	6	12	8	0
4	8	0	0	0
5	10	4	8	0
6	12	8	0	0
7	14	12	8	0
8	0	0	0	0
9	2	4	8	0
10	4	8	0	0
11	6	12	8	0
12	8	0	0	0
13	10	4	8	0
14	12	8	0	0
15	14	12	8	0

---

## 17

---

0	0	0	0	0	0	0	0
1	2	4	8	16	15	13	9
2	4	8	16	15	13	9	1
3	6	12	7	14	11	5	10
4	8	16	15	13	9	1	2
5	10	3	6	12	7	14	11
6	12	7	14	11	5	10	3
7	14	11	5	10	3	6	12
8	16	15	13	9	1	2	4
9	1	2	4	8	16	15	13
10	3	6	12	7	14	11	5
11	5	10	3	6	12	7	14
12	7	14	11	5	10	3	6
13	9	1	2	4	8	16	15
14	11	5	10	3	6	12	7
15	13	9	1	2	4	8	16
16	15	13	9	1	2	4	8

---

## 18

---

0	0	0	0	0	0	0
1	2	4	8	16	14	10
2	4	8	16	14	10	2
3	6	12	6	12	6	12
4	8	16	14	10	2	4
5	10	2	4	8	16	14
6	12	6	12	6	12	6
7	14	10	2	4	8	16
8	16	14	10	2	4	8
9	0	0	0	0	0	0
10	2	4	8	16	14	10
11	4	8	16	14	10	2
12	6	12	6	12	6	12
13	8	16	14	10	2	4
14	10	2	4	8	16	14
15	12	6	12	6	12	6
16	14	10	2	4	8	16
17	16	14	10	2	4	8

---

# 19

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	6	12	5	10	1	2	4	8	16	13	7	14	9	18	17	15	11
4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2
5	10	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12
6	12	5	10	1	2	4	8	16	13	7	14	9	18	17	15	11	3
7	14	9	18	17	15	11	3	6	12	5	10	1	2	4	8	16	13
8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2	4
9	18	17	15	11	3	6	12	5	10	1	2	4	8	16	13	7	14
10	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5
11	3	6	12	5	10	1	2	4	8	16	13	7	14	9	18	17	15
12	5	10	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6
13	7	14	9	18	17	15	11	3	6	12	5	10	1	2	4	8	16
14	9	18	17	15	11	3	6	12	5	10	1	2	4	8	16	13	7
15	11	3	6	12	5	10	1	2	4	8	16	13	7	14	9	18	17
16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2	4	8
17	15	11	3	6	12	5	10	1	2	4	8	16	13	7	14	9	18
18	17	15	11	3	6	12	5	10	1	2	4	8	16	13	7	14	9

## 20

---

0	0	0	0	0	0
1	2	4	8	16	12
2	4	8	16	12	4
3	6	12	4	8	16
4	8	16	12	4	8
5	10	0	0	0	0
6	12	4	8	16	12
7	14	8	16	12	4
8	16	12	4	8	16
9	18	16	12	4	8
10	0	0	0	0	0
11	2	4	8	16	12
12	4	8	16	12	4
13	6	12	4	8	16
14	8	16	12	4	8
15	10	0	0	0	0
16	12	4	8	16	12
17	14	8	16	12	4
18	16	12	4	8	16
19	18	16	12	4	8

---



## 21

---

0	0	0	0	0	0
1	2	4	8	16	11
2	4	8	16	11	1
3	6	12	3	6	12
4	8	16	11	1	2
5	10	20	19	17	13
6	12	3	6	12	3
7	14	7	14	7	14
8	16	11	1	2	4
9	18	15	9	18	15
10	20	19	17	13	5
11	1	2	4	8	16
12	3	6	12	3	6
13	5	10	20	19	17
14	7	14	7	14	7
15	9	18	15	9	18
16	11	1	2	4	8
17	13	5	10	20	19
18	15	9	18	15	9
19	17	13	5	10	20
20	19	17	13	5	10

---

---

0	0	0	0	0	0	0	0	0	0	0
1	2	4	8	16	10	20	18	14	6	12
2	4	8	16	10	20	18	14	6	12	2
3	6	12	2	4	8	16	10	20	18	14
4	8	16	10	20	18	14	6	12	2	4
5	10	20	18	14	6	12	2	4	8	16
6	12	2	4	8	16	10	20	18	14	6
7	14	6	12	2	4	8	16	10	20	18
8	16	10	20	18	14	6	12	2	4	8
9	18	14	6	12	2	4	8	16	10	20
10	20	18	14	6	12	2	4	8	16	10
11	0	0	0	0	0	0	0	0	0	0
12	2	4	8	16	10	20	18	14	6	12
13	4	8	16	10	20	18	14	6	12	2
14	6	12	2	4	8	16	10	20	18	14
15	8	16	10	20	18	14	6	12	2	4
16	10	20	18	14	6	12	2	4	8	16
17	12	2	4	8	16	10	20	18	14	6
18	14	6	12	2	4	8	16	10	20	18
19	16	10	20	18	14	6	12	2	4	8
20	18	14	6	12	2	4	8	16	10	20
21	20	18	14	6	12	2	4	8	16	10

---

## 23

---

0	0	0	0	0	0	0	0	0	0	0
1	2	4	8	16	9	18	13	3	6	12
2	4	8	16	9	18	13	3	6	12	1
3	6	12	1	2	4	8	16	9	18	13
4	8	16	9	18	13	3	6	12	1	2
5	10	20	17	11	22	21	19	15	7	14
6	12	1	2	4	8	16	9	18	13	3
7	14	5	10	20	17	11	22	21	19	15
8	16	9	18	13	3	6	12	1	2	4
9	18	13	3	6	12	1	2	4	8	16
10	20	17	11	22	21	19	15	7	14	5
11	22	21	19	15	7	14	5	10	20	17
12	1	2	4	8	16	9	18	13	3	6
13	3	6	12	1	2	4	8	16	9	18
14	5	10	20	17	11	22	21	19	15	7
15	7	14	5	10	20	17	11	22	21	19
16	9	18	13	3	6	12	1	2	4	8
17	11	22	21	19	15	7	14	5	10	20
18	13	3	6	12	1	2	4	8	16	9
19	15	7	14	5	10	20	17	11	22	21
20	17	11	22	21	19	15	7	14	5	10
21	19	15	7	14	5	10	20	17	11	22
22	21	19	15	7	14	5	10	20	17	11

---

## 24

---

0	0	0	0	0
1	2	4	8	16
2	4	8	16	8
3	6	12	0	0
4	8	16	8	16
5	10	20	16	8
6	12	0	0	0
7	14	4	8	16
8	16	8	16	8
9	18	12	0	0
10	20	16	8	16
11	22	20	16	8
12	0	0	0	0
13	2	4	8	16
14	4	8	16	8
15	6	12	0	0
16	8	16	8	16
17	10	20	16	8
18	12	0	0	0
19	14	4	8	16
20	16	8	16	8
21	18	12	0	0
22	20	16	8	16
23	22	20	16	8

---