Clock Squares

Mahdi Raza Khunt
Mahatma Gandhi International School

I created this table with the first two rows about the number and it's square. Then the following columns include the number mod prime such as 5, 7 , 11, 13 and 17 to test and observe any findings.

n	n^2	5	7	11	13	17
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	4	4	4	4	4
3	9	4	2	9	9	9
4	16	1	2	5	3	16
5	25	0	4	3	12	8
6	36	1	1	3	10	2
7	49	4	0	5	10	15
8	64	4	1	9	12	13
9	81	1	4	4	3	13
10	100	0	2	1	9	15
11	121	1	2	0	4	2
12	144	4	4	1	1	8
13	169	4	1	4	0	16
14	196	1	0	9	1	9
15	225	0	1	5	4	4
16	256	1	4	3	9	1
17	289	4	2	3	3	0
18	324	4	2	5	12	1
19	361	1	4	9	10	4

The very first thing I notice is how similar patterns emerge from n mod p and n^2 mod p. The values modulo prime numbers, also repeat in the same interval. So, for example, the column with 5 has remainders that repeat after every 5 integers. Same goes with 7, 11, 13 and 17. Also, excluding the zero, I noticed that the "block" (That is highlighted in bold for each column) is symmetrical from the top and bottom. Later I also figured out the reason behind this; Euclidean algorithm!

In general, let's say there is a positive integer 'a' which is modulo 'p'. From the Euclidean algorithm, we know that the possible values are 0, 1, 2, 3, all the way till (p - 1).
Thus, to represent in algebraic form, a can be of the form:

$$\begin{aligned} a &= 0 + k \cdot p \\ a &= 1 + k \cdot p \\ a &= 2 + k \cdot p \\ a &= 3 + k \cdot p \\ &\cdots \\ a &= p - 1 + k \cdot p \end{aligned}$$

When we square both sides, we get:

$$\begin{aligned} a^2 &= 0 + k \cdot p \\ a^2 &= 1 + k \cdot p \\ a^2 &= 4 + k \cdot p \\ a^2 &= 9 + k \cdot p \\ &\cdots \\ a^2 &= p^2 - 6p + 9 + k \cdot p \\ a^2 &= p^2 - 4p + 4 + k \cdot p \\ a^2 &= p^2 - 2p + 1 + k \cdot p \end{aligned}$$

Taking out p common from both sides:

$$\begin{aligned} a^2 &= 0 + p(k) \\ a^2 &= 1 + p(k) \\ a^2 &= 4 + p(k) \\ a^2 &= 9 + p(k) \\ &\cdots \\ a^2 &= 9 + p(p - 6 + k) \\ a^2 &= 4 + p(p - 4 + k) \\ a^2 &= 1 + p(p - 2 + k) \end{aligned}$$

Representing in modular form, we see that the values repeat from the bottom and top, which is the pattern of 1, 4, 9, ..., 9, 4, 1. This can be seen in module 11. The pattern also repeats periodically, similar to integers that are not raised to any power.

For modulo 5, we see that values of 0, 1, 4, 4 and 1 repeat.

Another concise way to represent this is $r^2 \equiv (p - r)^2 \mod p$.

$1 \equiv 1^2 \equiv 6^2 \equiv 11^2 \equiv 16^2 \equiv (5n + 1)^2 \mod 5$

Hence, $101^2 \equiv 1 \mod 5$. We can also verify that 101 squared is 10201 which leaves remainder of 1 when divided by 5.

Similarly, $102^2 \equiv 4 \mod 5$, $103^2 \equiv 4 \mod 5$, $104^2 \equiv 1 \mod 5$ and $105^2 \equiv 0 \mod 5$

n	n^2	2	4	6	8	18
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	0	0	4	4	4
3	9	1	1	3	1	9
4	16	0	0	4	0	16
5	25	1	1	1	1	7
6	36	0	0	0	4	0
7	49	1	1	1	1	13
8	64	0	0	4	0	10
9	81	1	1	3	1	9
10	100	0	0	4	4	10
11	121	1	1	1	1	13
12	144	0	0	0	0	0
13	169	1	1	1	1	7
14	196	0	0	4	4	16
15	225	1	1	3	1	9

My claim is that for every prime number, we require <u>at most</u> the first $\frac{p+1}{2}$ natural numbers (Why at most is explained below in the case of modulo 8). The values start repeating as observed and also explained on page 2 about the pattern using Euclid's algorithm. This also means that there are only these many distinct values and another value of 0 that repeats periodically.

And for non-prime numbers, we require the first $\frac{n}{2}$ natural numbers.

We always know that $0^2 \equiv 0 \mod n$ for number n.

But, $n^2 \equiv 0 \mod n$ as well because $n \equiv 0 \mod n$ and so $n \times n \equiv 0 \times 0 \mod n$

And also, when we square any multiple of n. $nk \times nk \equiv 0 \times 0 \mod n \implies (nk)^2 \equiv 0 \mod n$

I stopped here thinking that there are only three cases when the obtained value is 0. Once when the integer is 0, second when the integer is n itself and lastly any multiple of k.

But I noticed something interesting when I looked at the table of modulo 8 !! It included $4^2 \equiv 0 \mod 8$ which satisfies none of the three conditions that I thought of. I realised that for an integer k, for $k^2 \equiv 0 \mod n$, the total factors for n should be completely there in k^2. So, 8 = 2 x 2 x 2 and 4^2 = 2 x 2 x 2 x 2 which includes all factors of 8. But, see that the same is not true for 6 or 10. The value of 0 appears again after squaring a multiple of 4.

The same is observed in 18 as well. Values of $6^2 \equiv 12^2 \equiv 0 \mod 18$ appear even before $18^2 \equiv 0 \mod 18$.

So, <u>according to my observations</u>, the only possible cases when $x^2 \equiv 0 \mod n$ happens is in these four situations.