Problem Set 1: Integers Modulo n

1) Determine which elements have multiplicative inverses in the following sets of integers modulo n:

(a) $\mathbb{Z}_{12}$

Solution: An easy thing to do here is create a multiplication table and look for when a product of 1 is achieved. All products are reduced modulo 12.

$\mathbb{Z}_{12}$	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Therefore, the only invertible elements are $1, 5, 7, 11$. ■

(b) $\mathbb{Z}_3$

Solution:

$\mathbb{Z}_3$	1	2
1	1	2
2	2	1

Invertible elements: 1 and 2. ■

(c) $\mathbb{Z}_4$

Solution:

$\mathbb{Z}_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Invertible elements: 1 and 3. ■

(d) $\mathbb{Z}_5$

Solution:

$\mathbb{Z}_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Invertible elements: $1, 2, 3, 4$. ■

(e) $\mathbb{Z}_6$

Solution:

$\mathbb{Z}_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Invertible elements: 1 and 5. ■

(f) $\mathbb{Z}_7$

Solution:

$\mathbb{Z}_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Invertible elements: $1, 2, 3, 4, 5, 6$. ■

(g) $\mathbb{Z}_2$

Solution: The only non-zero element is 1, which is its own inverse! ■

(h) If every non-zero element a of $\mathbb{Z}_n$ has a multiplicative inverse, we say that $\mathbb{Z}_n$ is a **field**. Which of the above sets were fields? See any patterns?

Solution: The fields present are $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_7$. This occurs for $\mathbb{Z}_n$ when n is prime! ■

(i) How do the elements **without** inverses relate to the modulus? Have you noticed any patterns?

Solution: If you look through the tables, you should see that any non-invertible element has a common factor with a modulus! In other words, for $k \in \mathbb{Z}_n$ that is not invertible, we have that $\gcd(k, n) > 1$. ■

2) In $\mathbb{Z}_{12}$, we already saw that $-6 \equiv 6 \pmod{12}$, which is a really strange property to see! The only number in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ whose negative is equal to itself is 0.

(a) In which of the sets listed in Question **1)** can you find a non-zero number x such that $-x \equiv x \pmod{n}$?

Solution: There are two ways to check this. First, see if any element above satisfies $x \equiv -x \equiv n - x \pmod{n}$. However, with the multiplication tables, we have a quicker method! As $n - 1 \equiv -1 \pmod{n}$. we can simply check for the elements which are fixed in the final column of each table. Using this, we see that

$$2 \equiv -2 \pmod{4}$$
$$3 \equiv -3 \pmod{6}$$
$$1 \equiv -1 \pmod{2}.$$ ■

(b) Can you determine the necessary condition for $-x \equiv x \pmod{n}$ to be possible? Prove your condition works!

Solution: For $x \in \mathbb{Z}_n$, for $x \equiv n - x$, we simply need $x = n - x$. Solving for x, we have $2x = n$ or $x = \frac{n}{2}$. As x is an integer, we need n to be even! That's our condition - when n is even and x is half of n, we have $x \equiv -x \pmod{n}$. ■

3) For our standard calendar, there are 7 days in a week, 365 days in a year, and 366 days in a leap year.

(a) Determine the values of 365 and 366 modulo 7.

Solution: Using long division, we see that $365 = 52 \cdot 7 + 1$, thus

$$365 \equiv 1 \pmod{7} \text{ and } 366 = 365 + 1 \equiv 1 + 1 \equiv 2 \pmod{7}.$$ ■

(b) Today is Wednesday, October 30th, 2019. What day of the week will October 30th be in

(i) 2020?
(ii) 2021?
(iii) 2024?
(iv) 2030?

Solutions: We can think of each day of the week as a number modulo 7.

Set Sunday to 0, Monday to 1, Tuesday to 2, Wednesday to 3, Thursday to 4, Friday to 5, and Saturday to 6.

Then from October 30th, if the next year is not a leap year, we add 1 to the day of the week as 365 pass between October 30th in successive years, and $365 \equiv 1 \pmod 7$. If the next year is a leap year (i.e. the year number is a multiple of 4), 366 days pass, so 2 is added to the day of the week as $366 \equiv 2 \pmod 7$.

Therefore, as October 30th, 2019 is on a Wednesday and thus has a value of 3, we have

(i) October 30th, 2020 is a Friday as $3 + 2 \equiv 5 \pmod 7$.

(ii) October 30th, 2021 is a Saturday as $5 + 1 \equiv 6 \pmod 7$.

(iii) October 30th, 2024 is a Wednesday. There are two normal years and a leap year between October 30th in 2020 and 2024, so we have $6 + 2 + 2 = 11 \equiv 4 \pmod 7$.

(iv) October 30th, 2030 is also a Wednesday. There are five normal years and one leap year between October 30th in 2024 and 2030, so we have $3 + 5 + 2 = 3 + 7 \equiv 3 \pmod 7$. ■

(c) What is the first year in the future that will have the exact same calendar as 2019? By this, I mean that every day of the year falls on the same day of the week as it does in 2019, and has the same number of days.

Solution: In both 2024 and 2030, October 30th is a Wednesday, as it is in 2019. So if you trace back each previous day of the year, or forward each remaining day of the year, you should get the same days of the week as in 2019. However, 2024 is a leap year, so this won't work for days before March. Since 2030 is not a leap year, along with 2019, the first year with the exact same calendar after 2019 is 2030. (you can check that Oct 30this not a Wednesday in 2025-2029) ■

4) We have yet to consider square roots in $\mathbb{Z}_n$ (and will do so in great detail later!) For now, for the following sets, determine for which values a the equation $x^2 \equiv a \pmod n$ has a solution, and give all possible solutions when one exists!

Solutions: We'll abbreviate $x^2 \pmod n$ as $x^2\ (n)$.

(a) $\mathbb{Z}_5$:

x	0	1	2	3	4
$x^2\ (5)$	0	1	4	4	1

Therefore, 0, 1, and 4 are all squares mod 5. We have that 0 has one "square root" in $\mathbb{Z}_5$, and both 1 and 4 have two. ■

(b) $\mathbb{Z}_6$:

x	0	1	2	3	4	5
$x^2\ (6)$	0	1	4	3	4	1

Therefore, 0, 1, 3, and 4 are squares mod 6. We have that both 0 and 3 have one square root in $\mathbb{Z}_6$, and both 1 and 4 have two. ■

(c) $\mathbb{Z}_8$:

x	0	1	2	3	4	5	6	7
x^2 (8)	0	1	4	1	0	1	4	1

Therefore, 0, 1, and 4 are squares mod 8. We have that both 0 and 4 have two square roots in $\mathbb{Z}_8$, and 1 has four! ■

(d) $\mathbb{Z}_{10}$:

x	0	1	2	3	4	5	6	7	8	9
x^2 (10)	0	1	4	9	6	5	6	9	4	1

Therefore, 0, 1, 4, 5, 6 and 9 are squares mod 10. We have that both 0 and 5 have one square root in $\mathbb{Z}_{10}$, and the other squares have exactly 2 roots. ■

(e) When a solution exists, how many solutions do you get? Why does this happen?

Solution: The only discernable pattern here is that when a square and the modulus have no common factor (so $\gcd(a, n) = 1$), there are exactly two distinct square roots. ■