The Poison Game
The Poison Game is a two-player game where there are $N$ poison pills in front of the players. Each player can take 1 or 2 pills on their turn. The player whose turn it is when one pill is left has to take the poison pill and loses!

Let’s consider what happens as the number $N$ varies from 1 to 10 and try to see if we can find a pattern in who wins the game, Player One or Player Two, and how it depends on the number $N$ of pills in the pot and the strategies used by the player.

GROUPWORK
Play the Poison game with a varying number of pills and see if any patterns emerge.

Is there a winning strategy for either of the players?
Write down which player wins the poison game when \( N \) varies in the table below

<table>
<thead>
<tr>
<th>( N )</th>
<th>Number of pills</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>PATTERN 1</th>
<th>PATTERN 2</th>
<th>PATTERN 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winning Player</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Analyzing The Poison Game**

Q: What’s the simplest case?
A: \( N = 1 \).

Q: Who wins in this case?
A: ________________

Q: What’s the next simplest case?
A: \( N = 2 \).

Q: Who wins in this case?
A: ________________

Q: What’s the next simplest case?
A: \( N = 3 \).

Q: Who wins in this case?
A: ________________

Q: What’s the next simplest case?
A: \( N = 4 \).

Q: Who wins in this case?
A: Player 2 always wins!

Q: What’s the winning strategy in this case?
A: ________________________

Q: What’s the next simplest case?
A: \( N = 5 \).

Q: Who wins in this case?
A: Player 1 always wins!

Q: What’s the winning strategy in this case?
A: ________________________

Q: What’s the next simplest case?
A: \( N = 6 \).

Q: Who wins in this case?
A: Player 1 always wins!

Q: What’s the winning strategy in this case?
A: ________________________
Three Cases To Analyze
Case 1: \( N = 4, 7, 10, 13, 16, 19, \ldots = 3k + 1 \)
Case 2: \( N = 5, 8, 11, 14, 17, 20, \ldots = 3k + 2 \)
Case 3: \( N = 6, 9, 12, 15, 18, 21, \ldots = 3k + 3 \)

Equivalent Numbers
The fact that in our analysis of Poison we found out that games that had \( 3k + 1 \) pills, \( 3k + 2 \) pills and \( 3k + 3 \) pills were all the same, or that

\[
4 \equiv 7 \equiv 10 \equiv 13 \equiv 16 \equiv 19 \ldots
\]

is an example of modular arithmetic.

We would say mathematically that \( 7 \equiv 1 \pmod{3} \).

Similarly, we can say that \( 14 \equiv 2 \pmod{3} \) and \( 18 \equiv 3 \pmod{3} \)

**DEFINITION: modular arithmetic**

Given two positive integers \( a \) and \( b \), they are said to be congruent modulo \( n \) if the difference between \( a \) and \( b \) is an integer multiple of \( n \), or in other words \( n \) evenly divides \( a - b \). The number \( n \) is known as the **modulus** of the congruence. The notation we use is

\[
a = b \pmod{n}
\]

When we say “two numbers are congruent modulo 3” we know that the difference of the two numbers must be a multiple of 3. Thus we know that in modulo 3 instead of counting 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, … we count 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, …

**DEFINITION: residue**

The **modulo-\( n \) residue** of \( a \) is \( b \) when \( a \equiv b \pmod{n} \) and we know that \( 0 \leq b < n \).

We say that there are three residue classes modulo 3. In general, if your modulus is \( n \) there are \( n \) residues classes ranging from 0 to \( n - 1 \). These are the numbers 0, 1, 2, 3, 4, 5, \ldots, \( n - 1 \).

**Examples of Modular Arithmetic**

The most common example of modular arithmetic involves clocks and time. There are 60 seconds in a minute and 60 minutes in a hour, so the modulus is 60. We tell time in 12 hour shifts so the modulus is 12 in hours.

7 hours past 6 o’clock is not 13 o’clock, it is 1 o’clock.

\[13 \equiv 1 \pmod{12}\] or \[7 + 6 \equiv 1 \pmod{12}\]

20 minutes after one-quarter before the hour is the same thing as 5 after the hour

\[45 + 20 \equiv 5 \pmod{60}\]

**EXERCISE**

Try to evaluate the following using modular arithmetic

1. \( 6 + 8 \equiv ?? \pmod{3} \)
2. \( ?? \equiv 4 \pmod{3} \)
3. \( ?? \equiv 4 \pmod{7} \)
4. \( 9 + 6 \equiv ?? \pmod{5} \)
5. \( 9 + 6 \equiv ?? \pmod{4} \)
Modular Arithmetic Rules

Addition Using Modular Arithmetic
Given that \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \) then it is true that \( a + c \equiv (b + d) \pmod{n} \)

Subtraction Using Modular Arithmetic
Given that \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \) then it is true that \( a - c \equiv (b - d) \pmod{n} \)

Multiplication Using Modular Arithmetic
Given that \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \) then it is true that \( ac \equiv bd \pmod{n} \)

Exponentiation Using Modular Arithmetic
Given that \( a \equiv b \pmod{n} \) and \( p \) is a positive integer then it is true that \( a^p \equiv b^p \pmod{n} \)

[Group Work]
Let’s use modular arithmetic for find the last two digits (i.e. the tens and units digits) of \( 7^{1942} \) (HINT: The modulus need to use is 100!)

What are the residue classes of 7 (mod 100)?

What can we simplify the expression \( 7^{4k} \pmod{100} \) as?

Can we write 1942 as \( 4k + j \) where \( k \) and \( j \) are integers and \( j \) is 0, 1, 2 or 3? Do it!

So, what are the last two digits of \( 7^{1942} \)?