


Using a cipher disk for modular addition and subtraction

Overview. You will make a simple mod-26 calculator and use it to solve some modular arithmetic problems.

Things to do.

1. Obtain a blank cipher disk. Fill in the inner ring of blanks with the numbers 0 through 25 in order, going clockwise. Do the same with the outer ring of blanks.
2. In the “0” cell on the inner ring, draw a heavy arrow pointing out toward the outer ring: 
3. *To add two numbers:* In an addition problem, the two numbers to be added together are called the *addends*, and their sum is called the *sum*. To solve an addition problem with the cipher disk, line up the arrow on the inner ring with the first addend on the outer ring. Then find the second addend on the inner ring. The sum (modulo 26) is the number just above the second addend.

Try these computations:

$$\begin{array}{l} 10 + 22 \bmod 26 = \boxed{} \\ 19 + 18 \bmod 26 = \boxed{} \end{array}$$

$$\begin{array}{l} 4 + 19 \bmod 26 = \boxed{} \\ 7 + 16 \bmod 26 = \boxed{} \end{array}$$

$$\begin{array}{l} 18 + 9 \bmod 26 = \boxed{} \\ 5 + 22 \bmod 26 = \boxed{} \end{array}$$

4. *To subtract two numbers:* Each of the numbers in a subtraction problem also has a name. In the equation $7 - 5 = 2$, for example, the number 7 is the *minuend*, the number 5 is the *subtrahend*, and the number 2 is the *difference*. To solve a subtraction problem on the cipher disk, find the minuend on the outer ring and the subtrahend on the inner ring. Line up these two numbers. The arrow on the inner ring points to the difference.

Try these computations:

$$\begin{array}{l} 22 - 6 \bmod 26 = \boxed{} \\ 9 - 18 \bmod 26 = \boxed{} \end{array}$$

$$\begin{array}{l} 4 - 19 \bmod 26 = \boxed{} \\ 7 - 16 \bmod 26 = \boxed{} \end{array}$$

$$\begin{array}{l} 18 - 9 \bmod 26 = \boxed{} \\ 5 - 22 \bmod 26 = \boxed{} \end{array}$$