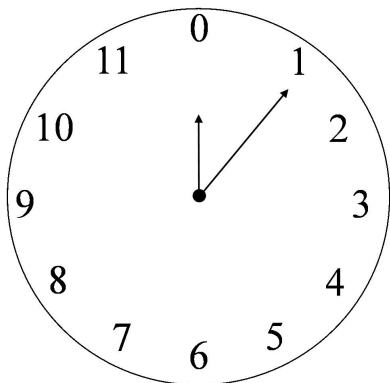
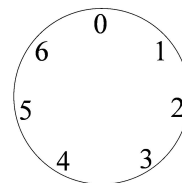


Modular Arithmetic Reference Sheet



Clock arithmetic: the integers modulo 12



“Seven hour clock” (integers $\text{mod } 7$)

Example.

- $5 \equiv 5 \text{ mod } 7$
- $12 \equiv 5 + 7 \equiv 5 + 0 \equiv 5 \text{ mod } 7$
- $5 + 12 \equiv 5 + 5 \equiv 10 \equiv 3 + 7 \equiv 3 \text{ mod } 7$

Definition. If a and b are two integers, and $a - b$ is divisible by m (i.e. $\frac{a-b}{m}$ is also an integer), then a and b are said to be *congruent modulo m* , and we write

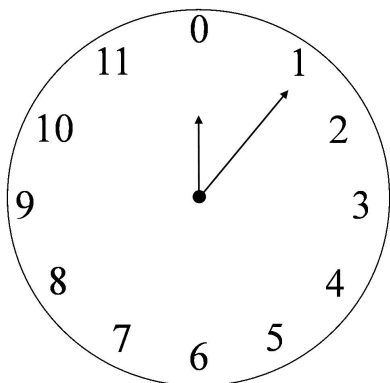
$$a \equiv b \text{ mod } m.$$

Example. Show that $-14 \equiv 2 \text{ mod } 16$.
So $a = -14$, $b = 2$, and $m = 16$. Then

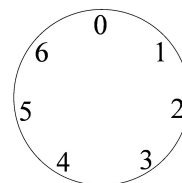
$$\frac{a-b}{m} = \frac{-14-2}{16} = \frac{-16}{16} = -1,$$

and -1 is an integer.

Modular Arithmetic Reference Sheet



Clock arithmetic: the integers modulo 12



“Seven hour clock” (integers $\text{mod } 7$)

Example.

- $5 \equiv 5 \text{ mod } 7$
- $12 \equiv 5 + 7 \equiv 5 + 0 \equiv 5 \text{ mod } 7$
- $5 + 12 \equiv 5 + 5 \equiv 10 \equiv 3 + 7 \equiv 3 \text{ mod } 7$

Definition. If a and b are two integers, and $a - b$ is divisible by m (i.e. $\frac{a-b}{m}$ is also an integer), then a and b are said to be *congruent modulo m* , and we write

$$a \equiv b \text{ mod } m.$$

Example. Show that $-14 \equiv 2 \text{ mod } 16$.
So $a = -14$, $b = 2$, and $m = 16$. Then

$$\frac{a-b}{m} = \frac{-14-2}{16} = \frac{-16}{16} = -1,$$

and -1 is an integer.