MOD Take 2: Additional Properties of Modular Arithmetic

The introductory MOD explainer noted two properties of modular arithmetic, *addition by a constant* and *multiplication by a constant*. This explainer provides some other useful properties of mod arithmetic that are encountered directly and indirectly throughout **PwP**. This explainer discusses this material in a bit more abstract fashion than in the introductory MOD explainer so do not worry if some of this sounds more abstract as well. We start with congruence.

Congruence. If the difference between two numbers $\boldsymbol{a}$ and $\boldsymbol{b}$ is divisible by a third number $\boldsymbol{m}$, $0 = \boldsymbol{a} - \boldsymbol{b}$ MOD $\boldsymbol{m}$, we say the two numbers are congruent modulo $\boldsymbol{m}$. This is written as $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$).

If you are not used to reading mathematical symbols you may not have noticed the three line ≡ congruence symbol (and read it as the two line = equality symbol) and you may wonder why the (MOD m) is shown with parentheses here. These distinctions are best explained by providing a concrete example. (One final distinction is that mathematicians use mod rather than MOD (capitals are used here as it is similar to Excel's MOD(a,b) function which is used throughout **PwP**).)

What time is it? Suppose it is now 12 o'clock. What time was it 11 hours ago? What time will it be 13 hours from now?

The answer to both questions is 1 o'clock. In mathematical terms:

$$-11 \equiv 13 \text{ (MOD 12)} \qquad \text{because} \qquad 0 = -11 - 13 \text{ MOD } 12 = -24 \text{ MOD } 12.$$

The (MOD 12) applies to both $\boldsymbol{a} = -11$ and $\boldsymbol{b} = 13$ so that $-11 \equiv 13$ (MOD 12) means -11 MOD 12 = 13 MOD 12.The expression on each side of the = sign equals 1 ($-11 = 1 - 1 \cdot 12$ or $1 = -11$ MOD 12 and $13 = 1 + 1 \cdot 12$ or $1 = 13$ MOD 12).

Note that we do not know the remainder in the above congruence. All we know is that $\boldsymbol{a}$ and $\boldsymbol{b}$ will have the **SAME** remainder upon division by $\boldsymbol{m}$. We see why the remainders must be the same by assuming this is not the case and deriving a contradiction based on that incorrect assumption.

> Assume $\boldsymbol{a} = \boldsymbol{r_a} + \boldsymbol{x} \cdot \boldsymbol{m}$ with $0 \le \boldsymbol{r_a} < \boldsymbol{m}$ and $\boldsymbol{x}$ an integer, $\boldsymbol{b} = \boldsymbol{r_b} + \boldsymbol{y} \cdot \boldsymbol{m}$ with $0 \le \boldsymbol{r_b} < \boldsymbol{m}$ and $\boldsymbol{y}$ an integer and $\boldsymbol{r_a} \ne \boldsymbol{r_b}$. Define $\boldsymbol{a}$ as the number with larger remainder so $\boldsymbol{r_a} - \boldsymbol{r_b} > 0$. Given this, $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{r_a} - \boldsymbol{r_b} + (\boldsymbol{x} - \boldsymbol{y}) \cdot \boldsymbol{m}$ with $0 < \boldsymbol{r_a} - \boldsymbol{r_b} < \boldsymbol{m}$. But this says that $\boldsymbol{a} - \boldsymbol{b}$ has a non-zero remainder upon division by $\boldsymbol{m}$, contradicting $0 = \boldsymbol{a} - \boldsymbol{b}$ MOD $\boldsymbol{m}$.

We say that $\boldsymbol{a}$ and $\boldsymbol{b}$ are in the same *residue class* MOD $\boldsymbol{m}$ if they have the same remainder upon division by $\boldsymbol{m}$.

Properties. Modular congruence has many properties in common with the more common notion of equality.

Let $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$ and $\boldsymbol{k}$ be integers. The modulus, $\boldsymbol{m}$, is an integer greater than 1. The following are true.

Reflexivity:	$\boldsymbol{a} \equiv \boldsymbol{a}$ (MOD $\boldsymbol{m}$)
Symmetry:	$\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$) if and only if $\boldsymbol{b} \equiv \boldsymbol{a}$ (MOD $\boldsymbol{m}$)
Transitivity:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$) and $\boldsymbol{b} \equiv \boldsymbol{c}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} \equiv \boldsymbol{c}$ (MOD $\boldsymbol{m}$)
Addition by a constant, $\boldsymbol{k}$:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} + \boldsymbol{k} \equiv \boldsymbol{b} + \boldsymbol{k}$ (MOD $\boldsymbol{m}$)
Multiplication by a constant, $\boldsymbol{k}$:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} \cdot \boldsymbol{k} \equiv \boldsymbol{b} \cdot \boldsymbol{k}$ (MOD $\boldsymbol{m}$)
Addition:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$) and $\boldsymbol{c} \equiv \boldsymbol{d}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d}$ (MOD $\boldsymbol{m}$)
Subtraction:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$) and $\boldsymbol{c} \equiv \boldsymbol{d}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} - \boldsymbol{c} \equiv \boldsymbol{b} - \boldsymbol{d}$ (MOD $\boldsymbol{m}$)
Multiplication:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$) and $\boldsymbol{c} \equiv \boldsymbol{d}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a} \cdot \boldsymbol{c} \equiv \boldsymbol{b} \cdot \boldsymbol{d}$ (MOD $\boldsymbol{m}$)
Exponentiation:	If $\boldsymbol{a} \equiv \boldsymbol{b}$ (MOD $\boldsymbol{m}$), then $\boldsymbol{a}^{\boldsymbol{k}} \equiv \boldsymbol{b}^{\boldsymbol{k}}$ (MOD $\boldsymbol{m}$) for non-negative $\boldsymbol{k}$

Two examples: My 21st birthday is on Tuesday. What day of the week will my 25th birthday be on? How about my 65th?

Answers. *For 25.* Each 4-year cycle has 1 leap year so $T_{days} = 3 \cdot 365 + 366$. Since $52 \cdot 7 = 364$, $1 = 365$ MOD 7, $2 = 366$ MOD 7 so, $5 = 3 \cdot 1 + 2 = 3 \cdot 365 + 366 = T_{days}$ (MOD 7) or your 25th will be on a Sunday (5 more than Tuesday). *For 65.* $65 = 21 + 4 \cdot 11$ so, $6 = 55 = 11 \cdot 5 = 11 \cdot T_{days}$ (MOD 7) so that your 65th birthday will be on a Monday (6 more than Tuesday).