

This miniproject asks you to investigate the concept of modular arithmetic and prove some results about it using mathematical induction. You will need the following information about modular arithmetic.

Consider two positive integers a and b . We say that a is equivalent to $b \bmod n$ if when you divide a by n and you divide b by n you get the same remainder. (The term “remainder” here is used in the same sense as it was when you learned how to divide in grade school.) Common practice is to have $b \in \{0, 1, 2, \dots, n-1\}$. The notation is

$$a \equiv b \pmod{n}.$$

For example, since $\frac{19}{4} = 4\text{R}3$, we have $19 \equiv 3 \pmod{4}$.

Recall that an even number is a number that is divisible by two. In other words, an even number is a number a such that $a \equiv 0 \pmod{2}$. An odd number is a number that is not divisible by two, or a number b such that $b \equiv 1 \pmod{2}$. Modular arithmetic basically extends the concepts of even/odd to when you are talking about division by some number other than two, and where (therefore) there are more than two possible categories.

If you are interested in further results of using modular arithmetic (including when dealing with negative integers) see Section 3.4.

Note that we use modular arithmetic, specifically mod 60, when we refer to the time of day as “20 after”. We also use it when measuring the size of angles in degree-minutes-seconds.

In the following, you may use the following fact (without proof):

$$a \equiv b \pmod{n} \quad \text{if and only if} \quad a - b \equiv 0 \pmod{n}.$$

- (a) Do problems #33–35 of Section 3.4 of the textbook.
- (b) Use induction to prove that for non-negative integers n we have $n^2 + n \equiv 0 \pmod{2}$.
- (c) Use induction to prove that for non-negative integers n we have $n^3 - n \equiv 0 \pmod{6}$.
- (d) Prove that for non-negative integers k if we have $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.