

Modular Arithmetic

When doing computations in modular arithmetic, organize your work so that intermediate results are kept small. If you're working in base k , your final result should be in the form $[n]$ where $0 \leq n < k$.

1. In $\mathbb{Z}_{15}$, what are some values in the congruence class of $[14]$.
2. In $\mathbb{Z}_{15}$, find the value of $[7] + [14] \times [3]$.
3. Find the first six powers of $[5]$ in $\mathbb{Z}_7$. That is, compute $[5]^1, [5]^2$, and so on up to $[5]^6$.
4. Calculate the value of $[9]^{12}$ in $\mathbb{Z}_{11}$. (Hint: try repeated squaring.)

Subset Proof

Do at least one of the following. Use the back of the page for extra space.

$$A = \{(p, q) \in \mathbb{R}^2 : p^2 + q^2 \leq 1\}$$

$$B = \{(x, y) \in \mathbb{R}^2 : |x| \leq 1, |y| \leq 1\}.$$

Prove that $A \subseteq B$, by choosing a representative element from the smaller set and showing that it is in the larger set.

or

Show that $(A - C) - (B - C) \subseteq (A - B)$ is true for any sets A , B , and C . Your proof should choose a representative element from the smaller set and show that it is in the larger set.