

High quality precise arguments are more important than just quantity.

1	2	3	4	5	6	7	8	B1	B2
/	/	/	/	/	/	/	/	/	/
25	15	30	30	30	25	25	20		

You may use the following theorems without having to prove them:

Thm. 6.4.1. If $a, b \in \mathbf{Z}$ are not both zero, then there exist $x, y \in \mathbf{Z}$ such that $\gcd(a, b) = xa + yb$.

Thm. 6.4.3. If $a, b \in \mathbf{Z}$ are relatively prime, $c \in \mathbf{Z}$, and $a \mid bc$, then $a \mid c$.

1. Precisely state the definitions of **FIVE** of the following:

a. subset, b. function, c. one-to-one, d. sequence, e. finite, f. maximal, g. largest.

2. State the “division algorithm”. (Carefully state all hypotheses. Define all symbols that you use.)

3. a. Suppose $f: A \mapsto B$ is a function from a set A to a set B , and $\{A_\alpha: \alpha \in \Lambda\}$ is an indexed collection of subsets of A . Show that $f(\bigcap_{\alpha \in \Lambda} A_\alpha) \subseteq \bigcap_{\alpha \in \Lambda} f(A_\alpha)$.

b. Give an example of sets A, B, Λ, A_α and a function f for which $f(\bigcap_{\alpha \in \Lambda} A_\alpha) \not\subseteq \bigcap_{\alpha \in \Lambda} f(A_\alpha)$.

4. Suppose A, B and C are sets and $g: A \mapsto B$ and $f: B \mapsto C$ are functions.

a. Suppose that both f and g are one-to-one. Show that the composition $f \circ g$ is one-to-one.

b. Suppose $f \circ g$ is one-to-one. What can you conclude about f or g (or both)? Prove your result.

5. Suppose $f: A \mapsto A$ is a function from a set A to itself. For $n \in \mathbf{Z}^+$ let $f^{(n)}$ denote the $(n - 1)$ -fold composition of f with itself, defined recursively by $f^1 = f$, and $f^{(n+1)} = f \circ f^{(n)}$.

Use problem 4. and induction to prove: If f is one-to-one then $f^{(n)}$ is one-to-one for every $n \in \mathbf{Z}^+$.

6. a. Prove: If n is a natural number and n^2 is divisible by 6, then n is divisible by 6.

b. Show that there does not exist any rational number x such that $x^2 = 6$. (Hint: For an indirect proof, assume there exist integers p, q with $\gcd(p, q) = 1$ such that $(\frac{p}{q})^2 = 6$. Use part a.)

7. Let $n \in \mathbf{Z}^+$ and consider the relation \sim on \mathbf{Z} that is defined by $x \sim y$ if and only if the difference $(y - x)$ is a multiple of n (written $n \mid (y - x)$).

Show that \sim is an equivalence relation on \mathbf{Z} .

8. For the relation \sim of 7. show that if $a, a', b, b' \in \mathbf{A}$, $a \sim a'$ and $b \sim b'$ then $a \cdot b \sim a' \cdot b'$.

(Or, for less credit, show that, under the same hypotheses, $a + b \sim a' + b'$.)

Bonus. Prove by induction that for all $n \in \mathbf{Z}^+$, $n^n \geq n!$

Recall, the factorial is defined recursively by $1! = 1$ and $(n + 1)! = (n + 1) \cdot n!$ for $n \in \mathbf{Z}^+$.

Bonus. For the relation \sim of 7. denote by $\bar{m} = \{x \in \mathbf{Z}: x \sim m\}$ the equivalence class of $m \in \mathbf{Z}$.

Find all solutions of the linear equation $\bar{3} = \bar{6} \cdot \bar{x}$ in $\mathbf{Z}_7, \mathbf{Z}_8$, and in \mathbf{Z}_9 ,

i.e., solve the congruences $6 \cdot x \equiv 3 \pmod{m}$ where $m = 7, 8, 9$.