

Question 1. [¹⁰ pts each] Mark each of the following statements True or False and briefly explain each of your answers (one or two sentences). Complete proofs are not required.

- (a) The compound proposition $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is a tautology.

True, because the inference $p \rightarrow r$ from premises $p \rightarrow q$ and $q \rightarrow r$ is a valid rule of inference. [Or: make a truth table and check.]

- (b) If x and y are irrational real numbers, then $x + y$ is irrational.

False. One possible counterexample is $x = \sqrt{2}$, $y = -\sqrt{2}$, $x + y = 0$.

- (c) For every integer n there is a unique integer m such that $0 \leq m \leq 5$ and $m \equiv n \pmod{5}$.

False, because m exists but is not unique. For example, if $n=5$, then $m=0$ and $m=5$ are both solutions.

- (d) The set of prime numbers ~~is~~ countably infinite.

True. Proved in the book and in class to be infinite. Has to be countable because it is a subset of \mathbb{Z}^+ .

Question 2. (a) [10 pts] Prove or disprove: if A , B and C are sets, and $B \subseteq C$, then

$$(A \cup B) \cap C = (A \cap C) \cup B.$$

Proof ① To show $(A \cup B) \cap C \subseteq (A \cap C) \cup B$, let $x \in (A \cup B) \cap C$.

Then $x \in C$, and either $x \in A$ or $x \in B$. If $x \in A$, then $x \in A \cap C \subseteq (A \cap C) \cup B$. If $x \in B$, then again $x \in (A \cap C) \cup B$.

② To show $(A \cup B) \cap C \supseteq (A \cap C) \cup B$ let $x \in (A \cap C) \cup B$.

Then $x \in B$ or $x \in A \cap C$. If $x \in B$, then $x \in A \cup B$, and $B \subseteq C$ implies $x \in C$, so $x \in (A \cup B) \cap C$. If $x \in A \cap C$, then $x \in A \subseteq A \cup B$ and $x \in C$, so $x \in (A \cup B) \cap C$.

(b) [10 pts] Prove or disprove: the same identity as in part (a) for arbitrary sets A , B and C , when we do not assume that $B \subseteq C$.

The identity is false without assuming $B \subseteq C$, although the containment $(A \cup B) \cap C \subseteq (A \cap C) \cup B$ is still true, as part ① of the proof above shows.

For a counterexample, we can take $B = \{1\}$, $C = \emptyset$, and any set A that we like. Then

$$(A \cup B) \cap C = \emptyset$$

$$(A \cap C) \cup B = \{1\}.$$

Question 3. [16 pts] Compute $2^{100} \bmod 7$, showing enough work to justify your answer. Hint: first compute $2^3 \bmod 7$.

$$2^3 = 8 \equiv 1 \pmod{7}$$

$$2^{99} = (2^3)^{33} \equiv 1^{33} \equiv 1 \pmod{7}$$

$$2^{100} = 2 \cdot 2^{99} \equiv 2 \pmod{7}.$$

Since $0 \leq 2 < 7$, this shows that $\underline{2^{100} \bmod 7 = 2}$.

Question 4. [20 pts] Prove that if an integer n is a sum of two squares, then $n \not\equiv 3 \pmod{4}$. Of course, 'square' in this question means the square of an integer.

The simplest method is to compute

$$0^2 \equiv 2^2 \equiv 0 \pmod{4}$$

$$1^2 \equiv 3^2 \equiv 1 \pmod{4},$$

hence every square is \equiv to 0 or 1 $(\text{mod } 4)$.

If n is a sum of two squares, it follows that n is \equiv to $0+0=0$, $0+1=1$, or $1+1=2 \pmod{4}$, and therefore $n \not\equiv 3 \pmod{4}$.

A somewhat more complicated alternative is to let $n = k^2 + l^2$ and consider each case when k or l is even or odd.