

Problem 1: (a) Build a truth table with columns for $p \rightarrow q$, $p \wedge (p \rightarrow q)$, and so forth to determine whether $(p \wedge (p \rightarrow q)) \rightarrow q$ is a tautology. Explain why your answer is intuitively reasonable.

(b) Verify the result of (a) by applying logical equivalences. State which equivalence you are using at each step.

(c) Prove that for any sets A , B and C we always have

$$A \cap (\bar{A} \cup B) \subset B.$$

Solution: (a) A compound proposition, which depends on propositions p , q , r and so forth, is a tautology when it evaluates to true for any values of the propositions p , q and so forth. Intuitively, if we know p is true and p implies q when true, then we know that q is true. The truth table reads

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

(b) By definition of implication, the given statement is equivalent to

$$\neg(p \wedge (\neg p \vee q)) \vee q$$

which by de Morgan is equivalent to

$$\neg p \vee (p \wedge \neg q) \vee q.$$

Distributing each single-variable over each and gives

$$(((\neg p \vee p) \wedge (p \vee \neg q))) \vee q.$$

Excluded middle and domination simplify the expression to

$$p \vee \neg q \vee q$$

by associativity of \vee , which reduces to T by associativity, excluded middle and domination.

(c) Translate the previous logical statement into sets and quantify.

Problem 2: Define $\mathbf{Z}^+ = \{1, 2, 3, \dots\}$ and

$$\mathbf{Q}^+ = \{p/q \mid p \in \mathbf{Z}^+ \wedge q \in \mathbf{Z}^+ \wedge \gcd(p, q) = 1\}.$$

Define $f : \mathbf{Q}^+ \rightarrow \mathbf{Z}^+$ by $f(p/q) = p + q - 1$. Justify your answers to the following questions.

(a) Is f onto?

(b) Do \mathbf{Z}^+ and \mathbf{Q}^+ have the same cardinality?

Solution: (a) Every element n of \mathbf{Z}^+ is given by $n = f(p/q)$ for $p/q = n/1 \in \mathbf{Q}^+$. Hence $\boxed{f \text{ is onto.}}$ (Since $f(5/3) = f(3/5) = 8$, f is not one-to-one.)

(b) Since \mathbf{Z}^+ is \mathbf{N} with 0 removed, it is infinite and countable. We know that the rationals are countable, and a (bijective image of a) subset of a countable set is countable, so \mathbf{Q}^+ is countable. Since it contains \mathbf{Z}^+ , it is infinite, so

$\boxed{\mathbf{Z}^+ \text{ and } \mathbf{Q}^+ \text{ have the same cardinality.}}$

Problem 3: (a) Compute $(7 \times 11 \times 711 \times 777) \pmod{13}$ by modular arithmetic.
(b) Compute $666^{77} \pmod{11}$.

Solution: (a) Since $711 \equiv 61 \equiv -4 \pmod{13}$ and $777 \equiv -3 \pmod{13}$ we have

$$7 \times -2 \times -4 \times -3 \equiv -14 \times 12 \equiv -12 \equiv 1 \pmod{13}.$$

(b) Since $666 \equiv 6 \pmod{11}$, $666^{77} \equiv 6^{77} \pmod{11}$. The relevant powers of 6 (mod 11) are $6^2 = 36 \equiv 3$, $6^4 = 9$, $6^8 = 81 \equiv 4$, $6^{16} = 16 \equiv 5$, $6^{32} = 25 \equiv 3$, $6^{64} = 9$, and $77 = 64 + 8 + 4 + 1$ so $6^{77} \equiv 9 \times 4 \times 9 \times 6 \equiv 3 \times -1 \equiv -3 \equiv 8 \pmod{11}$. Alternatively, $6^{77} = (6^7)^{11} \equiv (9 \times 3 \times 6)^{11} \equiv 8^{11} = 2^{33} = 32^6 \times 8 \equiv 8 \pmod{11}$.

Problem 4: Consider the following pseudocode:

```
 $G(n \in \mathbf{N}, m \in \mathbf{N}, \text{function } f : \{0, 1, 2, \dots, n - 1\} \rightarrow \{0, 1, 2, \dots, m - 1\})$ 
  for  $i := 0$  to  $m - 1$ 
     $h_i := 0$ 
  end
  for  $j := 0$  to  $n - 1$ 
     $i := f(j)$ 
     $h_i := h_i + 1$ 
  end
  for  $i := 0$  to  $m - 1$ 
    if ( $h_i \neq 1$ ) then return F
  end
  return T
end
```

- (a) What function of f , n and m does G return?
(b) What is its worst-case complexity in terms of m and n in big- O notation? Justify your answer.
(c) Let $n = m > 2$. For what values of $a \in \mathbf{Z}$ does G return **T** for the function f defined by $f(j) = aj \bmod n$?

Solution: (a) It returns **T** iff the input function f is a bijection (a one-to-one correspondence).

(b) The worst-case complexity is $W(m, n) = O(m + n)$.

(c) This function is a bijection when a is invertible \pmod{n} , which happens when $\gcd(a, n) = 1$. Note: on the actual exam, the sets were $\{1, \dots, n\}$ and $\{1, \dots, m\}$ so this function was (a) not a function into the desired range and (b) never a bijection, since n was not in the range of $aj \bmod n$. Hence the answer “never” was also accepted as correct.