

## Math 55: First Midterm — Solutions

**Problem 1:** Prove that  $(p \wedge q) \rightarrow p$  is a tautology.

**Solution:**

$$\begin{aligned} & (p \wedge q) \rightarrow p \\ \Leftrightarrow & \neg(p \wedge q) \vee p && \text{Definition of implication} \\ \Leftrightarrow & (\neg p \vee \neg q) \vee p && \text{De Morgan} \\ \Leftrightarrow & \neg p \vee \neg q \vee p && \text{Associativity} \\ \Leftrightarrow & \neg p \vee p \vee \neg q && \text{Commutativity} \\ \Leftrightarrow & (\neg p \vee p) \vee \neg q && \text{Associativity again} \\ \Leftrightarrow & T \vee \neg q && \text{Excluded middle} \\ \Leftrightarrow & T && \text{Domination} \end{aligned}$$

**Problem 2:** Let  $f$ ,  $g$  and  $h$  be defined by:

$$\begin{aligned} f : \mathbf{R} &\rightarrow \mathbf{R}, & f(x) &= x^3 \\ g : \mathbf{Z} &\rightarrow \mathbf{Z}, & g(n) &= n^3 \\ h : \mathbf{R} &\rightarrow \mathbf{Z} \times \mathbf{Z}, & h(x) &= (\lfloor x \rfloor, \lceil x \rceil) \end{aligned}$$

For each of the functions  $f$ ,  $g$  and  $h$ , state whether the function is 1-1, whether it is onto, and whether it is invertible.

**Solution:** Since every real number  $x$  has a unique cube root  $\sqrt[3]{x}$ ,  $f$  is 1-1 and onto and therefore invertible.

Since not every integer is a cube (for example,  $2 = n^3$  implies  $n$  is between 1 and 2 so  $n \notin \mathbf{Z}$ ),  $g$  is not onto. However,  $n^3 = m^3$  implies  $m = n$ , so  $g$  is 1-1. Since  $g$  is not onto, it is not invertible.

Since  $x = 1/2$  and  $x = 1/4$  are both mapped to  $h(x) = (0, 1)$ ,  $h$  is not 1-1. Since  $(0, 100) \neq (\lfloor x \rfloor, \lceil x \rceil)$  for any  $x \in \mathbf{R}$ ,  $h$  is not onto. Since  $h$  is not 1-1 and not onto it is certainly not invertible.

**Problem 3:** Show that

$$\sum_{k=1}^n k^2 = O(n^3).$$

**Solution:**

$$\sum_{k=1}^n k^2 = 1 + 4 + 9 + \cdots + n^2 \leq n^2 + n^2 + \cdots + n^2 = n^3 = O(n^3).$$

**Problem 4:** Construct pseudocode for an algorithm which accepts input consisting of two finite sets  $A = \{a_1, a_2, \dots, a_n\}$  and  $B = \{b_1, b_2, \dots, b_m\}$  and a function  $f : A \rightarrow B$ , and returns output  $T$  if  $f$  is onto and  $F$  if  $f$  is not onto.

**Solution:**

```

Boolean function onto( set A, set B, function f : A → B ):
for b ∈ B
    hit := F
    for a ∈ A
        if (b = f(a)) hit := T
    if (hit = F) return(onto := F)
return(onto := T)

```

**Problem 5:** Suppose  $a \equiv b$  and  $c \equiv d \pmod{17}$ . Show that  $ac \equiv bd \pmod{17}$ .

**Solution:** By definition of “mod,” there are integers  $p$  and  $q$  such that  $a = b + 17p$  and  $c = d + 17q$ . Then

$$ac - bd = (b + 17p)(d + 17q) - bd = (pq + pd + qb)17 \equiv 0 \pmod{17}.$$

By definition,  $ac \equiv bd \pmod{17}$ .

**Problem 6:** Use the Euclidean algorithm to compute  $\gcd(277, 123)$ .

**Solution:**

	$x = 277$	$y = 123$
$r = 277 \pmod{123} = 31$	$x = 123$	$y = 31$
$r = 123 \pmod{31} = 30$	$x = 31$	$y = 30$
$r = 31 \pmod{30} = 1$	$x = 30$	$y = 1$
$r = 30 \pmod{1} = 0$	$x = 1 = \gcd(277, 123)$	$y = 0$

**Problem 7:** Suppose  $x$  is an integer with  $0 \leq x \leq 1000$  and

$$x \pmod{7} = 3, \quad x \pmod{11} = 5, \quad x \pmod{13} = 7.$$

(a) Is  $x$  uniquely determined by this information? Why or why not?

**Solution:** Yes, by the Chinese Remainder Theorem, because 7, 11 and 13 are pairwise relatively prime and  $7 \cdot 11 \cdot 13 = 1001$ .

(b) Calculate  $x^2 \pmod{7}$  and  $x^3 \pmod{11}$ .

**Solution:**

$$x^2 \pmod{7} = (x \pmod{7})^2 = 9 \equiv 2 \pmod{7}$$

$$x^3 \pmod{11} = (x \pmod{11})^3 = 125 \equiv 4 \pmod{11}$$