Solutions to Mini-Quiz Apr. 7

Problem 1 (8 points). (a) Use the Pulverizer to find $gcd(84, 108)$

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
108	84	24	$=$	$1 \cdot 108 - 1 \cdot 84$
84	24	12	$=$	$-3 \cdot 108 + 4 \cdot 84$
24	12	0		

■

(b) Find integers x, y with $0 \leq y < 84$ such that

$$x \cdot 84 + y \cdot 108 = \gcd(84, 108).$$

Solution. From the table above,

$$4 \cdot 84 - 3 \cdot 108 = \gcd(84, 108).$$

Therefore,

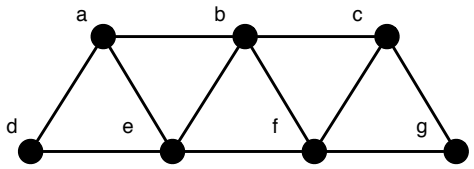
$$(4 - 108 \cdot k) \cdot 84 + (-3 + 84 \cdot k) \cdot 108 = \gcd(84, 108).$$

So, letting $k = 1$, $(x, y) = (4 - 108 \cdot 1, -3 + 84 \cdot 1) = (-104, 81)$ works. ■

(c) Find the multiplicative inverse of 84 modulo 108 in the range {1,...,107}. If no such inverse can be found, briefly explain why not.

Solution. There is no inverse of 84 modulo 108. The inverse of a modulo m exists iff $gcd(a, m) = 1$. Clearly $gcd(84, 108) = 12 \neq 1$, so there is no inverse of 84 modulo 108. ■

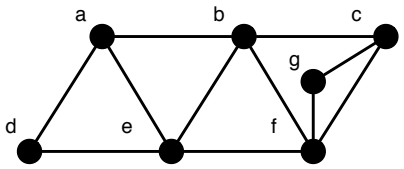
Problem 2 (6 points). (a) For the planar embedding picture below, list all the discrete faces (simple cycles that define the region borders).



Solution. adea, abea, befb, bcfb, cfgc, abcgfeda ■

(b) Provide a drawing of a different planar embedding of the graph above. Also list all the faces of the embedding.

Solution. The planar drawing below has the following faces: adea, abea, befb, bcgfb, cfgc, abcfeda



■

Problem 3 (6 points).

Definition. Consider a new recursive definition, MB_0, of the same set of "matching" brackets strings as MB (definition of MB is provided in the Appendix):

- **Base case:** $\lambda \in \text{MB}_0$.
- **Constructor cases:**
  - (i) If s is in MB_0, then $[s]$ is in MB_0.
  - (ii) If $s, t \in \text{MB}_0$, $s \neq \lambda$, and $t \neq \lambda$, then st is in MB_0.

(a) Suppose structural induction was being used to prove that $\text{MB}_0 \subseteq \text{MB}$. Circle the one predicate below that would fit the format for a structural induction hypothesis in such a proof.

- $P_0(n) ::= |s| \leq n$ IMPLIES $s \in \text{MB}$.
- $P_1(n) ::= |s| \leq n$ IMPLIES $s \in \text{MB}_0$.
- $P_2(s) ::= s \in \text{MB}$.
- $P_3(s) ::= s \in \text{MB}_0$.
- $P_4(s) ::= (s \in \text{MB}$ IMPLIES $s \in \text{MB}_0)$.

Solution. $\text{MB}_0 \subseteq \text{MB}$ means that $\forall s \in \text{MB}_0.\ s \in \text{MB}$. To prove this, the only hypothesis above that fits the format for a structural induction would be P_2 in a structural induction on the definition of MB_0. ■

(b) The recursive definition MB_0 is *ambiguous*. Verify this by giving two different derivations for the string "[ ][ ][ ]" according to MB_0.

Solution. MB_0 is ambiguous because "[ ][ ][ ]" $\in \text{MB}_0$ can be derived from the second constructor with $s = [\,]$ and $t = [\,][\,]$, but also with $s = [\,][\,]$ and $t = [\,]$. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010