Solution to Graded Problem Set 6

Date: 25.10.2013 Due date: 1.11.2013, noon

Problem 1.

(a) The functions $g_i : \mathbb{N} \to \mathbb{R}^+$ $(i = 1, 2)$ are $\Theta(f)$ for some function f. So there exist $c_{i,j} > 0$ and $k_i > 0$ $(j = 1, 2)$ s.t.

$$c_{i,1}|f(x)| \leq |g_i(x)| \leq c_{i,2}|f(x)| \qquad \forall x > k_i.$$

Set $k = \max_i k_i$. Then, for all $x > k$,

$$c_{1,1}|f(x)| \leq |g_1(x)| \leq c_{1,2}|f(x)| \quad \text{and} \quad c_{2,1}|f(x)| \leq |g_2(x)| \leq c_{2,2}|f(x)|.$$

Consequently,

$$(c_{1,1} + c_{2,1})|f(x)| \leq |g_1(x)| + |g_2(x)| \leq (c_{1,2} + c_{2,2})|f(x)|.$$

The triangle inequality tells us that $|g_1(x)+g_2(x)| \leq |g_1(x)|+|g_2(x)|$. Defining $c_2 = c_{1,2}+c_{2,2}$, we have that $|g_1(x) + g_2(x)| \leq c_2|f(x)|$. Therefore, we can conclude that $g_1 + g_2$ is $O(f)$. Since $g_i : \mathbb{N} \to \mathbb{R}^+$, $|g_1(x) + g_2(x)| = |g_1(x)| + |g_2(x)| = g_1(x) + g_2(x)$ and we obtain that

$$c_1|f(x)| \leq |g_1(x) + g_2(x)|,$$

where $c_1 = c_{1,1} + c_{2,1}$. As a result, $g_1 + g_2$ is $\Omega(f)$. Since $g_1 + g_2$ is also $O(f)$, by definition we find that $g_1 + g_2$ is $\Theta(f)$.

(b) We use the same notation as in (a) and we obtain that for all $x > k$,

$$(c_{1,1} \cdot c_{2,1})f^2(x) \leq |g_1(x)| \cdot |g_2(x)| \leq (c_{1,2} \cdot c_{2,2})f^2(x).$$

Let $c_j = c_{1,j} \cdot c_{2,j}$. As $|g_1(x)g_2(x)| = |g_1(x)||g_2(x)|$,

$$c_1 f^2(x) \leq |(g_1 \cdot g_2)(x)| \leq c_2 f^2(x), \qquad \forall x > k,$$

which implies that $g_1 \cdot g_2$ is $\Theta(f^2)$.

(c) In this case, the functions g_3, g_4 may take negative values. We can follow the reasoning in (a) to show that $g_3 + g_4$ is $O(f)$. But there exist g_3, g_4 s.t. $g_3 + g_4$ is not $\Omega(f)$. For instance, let $g_4(x) = -g_3(x)$. Then, $(g_3 + g_4)(x) = 0$. Consequently $\forall c > 0$, $\forall x > 0$, we have that $|g_3(x) + g_4(x)| = 0 < c|f(x)|$ for any non-zero function $f : \mathbb{N} \to \mathbb{R}^+$. As a consequence $g_3 + g_4$ is not $\Omega(f)$ and the statement is false.

(d) The statement is true and the proof is the same as in (b).

Problem 2.

(a) Pick

$$f(n) = \begin{cases} \dfrac{1}{n} & n \text{ even} \\ n^n & n \text{ odd} \end{cases}$$

Indeed, on the even numbers $f(n)$ is NOT $\Omega(n)$ and on the odd numbers $f(n)$ is not $o(e^n)$.

(b) (i) Recall that $n! = \Omega(a^n)$ for any fixed $a \in \mathbb{R}$. Let $a = 2^{2013}$, then

$$(\lceil \log_2 n \rceil)! = \Omega((2^{2013})^{\log_2 n}) = \Omega(n^{2013}).$$

(ii) Recall that $n! \leq n^n$. Hence,

$$(\lceil \log_2 n \rceil)! \leq (\log_2 n)^{\log_2 n} = 2^{\log_2 n \cdot \log_2 \log_2 n} \leq 2^{(\log_2 n)^2}.$$

Since $(\log_2 n)^2$ is $o(n)$, the result follows.

Problem 3. Take $\mathcal{C} = \{f^{(\alpha)} : \alpha \in (0,1)\}$, where $f^{(\alpha)}(n) = n(\log n)^{46+\alpha}$. The three required conditions are satisfied:

(i)-(ii) For any $\alpha, \beta \in [0,1]$ with $\alpha < \beta$, we have $f^{(\alpha)} = o(f^{(\beta)})$ because

$$\lim_{n\to\infty} \frac{f^{(\alpha)}(n)}{f^{(\beta)}(n)} = \lim_{n\to\infty} \frac{n \cdot (\log n)^{46+\alpha}}{n \cdot (\log n)^{46+\beta}} = \lim_{n\to\infty} \frac{1}{(\log n)^{\beta-\alpha}} = 0.$$

As a result, condition (ii) is satisfied. Setting $\beta = 1$, we have that $f^{(\alpha)} = o(n \cdot (\log n)^{47})$ for any $\alpha \in (0,1)$. In addition, setting $\alpha = 0$, we obtain that $f^{(\beta)} = \Omega(n \cdot (\log n)^{46})$ for any $\beta \in (0,1)$. These two observations prove that condition (i) is fulfilled.

(iii) Consider the function $h : (0,1) \to \mathcal{C}$, defined as $h(\alpha) = f^{(\alpha)}$. This is clearly a bijection and therefore $|\mathcal{C}| = |(0,1)|$. To show that $|(0,1)| = |\mathbb{R}|$, it is enough to consider a function similar to that of the solution of Problem 4(b) in Homework 4. Indeed, let $g : \mathbb{R} \to (0,1)$ be defined as

$$g(x) = \frac{\dfrac{e^x - e^{-x}}{e^x + e^{-x}} + 1}{2}.$$

Then, g is bijective and thus $|(0,1)| = |\mathbb{R}|$.

Problem 4.

(i) False. Indeed, pick $a = b = c = 1$ and $d = 2$. Then, $1 \mid 1$ and $1 \mid 2$, but $2 \nmid 3$.

(ii) True. Indeed, if $a \mid b$, then $\exists k \in \mathbb{Z} : b = ka$. Analogously, if $b \mid c$, then $\exists l \in \mathbb{Z} : c = lb$. Consequently, $c = lb = lka$, which means that $a \mid c$.

(iii) False. Indeed, pick $a = b = c = 1$. Then, $1 \mid 1$ and $1 \mid 1$, but $2 \nmid 1$.

(iv) False. Indeed, pick $a = b = 2$, $c = d = 1$. Then, $2 \mid 2$ and $1 \mid 1$, but $2 \nmid 3$.

(v) True. Indeed, let $a, b \in \mathbb{N}$. Then, if $a \mid b$, then $\exists k \in \mathbb{N} : b = ka$. If $b \mid a$, then $\exists k' \in \mathbb{N} : a = k'b$. As a result, $b = kk'b$, which implies that $k = k' = 1$. Therefore, $a = b$.

(vi) False. Indeed, pick $a = 1$ and $b = -1$. Then, $a \mid b$ and $b \mid a$, but $a \neq b$.

(vii) False. Indeed, pick $a = 2$, and $b = c = 3$. Then, $2 \mid 6$, but $2 \nmid 3$.

(viii) False. Indeed, pick $a = 4$, $b = 2$, and $c = 6$. Then, $4 \mid 12$, but $4 \nmid 2$ and $4 \nmid 6$.

(ix) True. Indeed, if $a \mid c$, then $\exists k \in \mathbb{Z} : c = ka$. If $b \mid c$, then $\exists l \in \mathbb{Z} : c = lb$. Consequently, $c^2 = klab$, which implies that $ab \mid c^2$.

(x) True. Indeed, by the existence of the unique factorization, write $b = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ and $c = p_1^{j_1} \cdot \ldots \cdot p_n^{j_n}$, where one of k_i and j_i can be zero, but not both for all $1 \leq i \leq n$. Then $bc = p_1^{k_1+j_1} \cdot \ldots \cdot p_n^{k_n+j_n}$. Since $a \mid bc$ and a is a positive prime, there must be $i \in \{1, \ldots, n\}$ s.t. $a = p_i$. Either k_i or j_i is positive, so either $a \mid p_i^{k_i}$ or $a \mid p_i^{j_i}$, which means that either $a \mid b$ or $a \mid c$.

Problem 5.

(i) If a and p are not coprime, then it must be that $p \mid a$. In this case, $a \equiv 0 \pmod p$ and $a^p \equiv 0 \pmod p$. Consequently, $a^p \equiv a \pmod p$.

(ii) Consider now a such that $\gcd(a, p) = 1$. Then $p \nmid a$ and for any $k \in \{1, \ldots, p-1\}$ also $p \nmid ak$. Using the converse of the statement Problem 4(x) of the current problem set, we obtain $ak \not\equiv 0 \pmod p$ and thus $\mathcal{A} \subseteq \{1, \ldots, p-1\}$ (we used the fact that $\mathcal{A}$ is a set of reminders).

To prove that $\mathcal{A} \supseteq \{1, \ldots, p-1\}$, we just need to show that for any k, $k' \in \{1, \ldots, p-1\}$ the corresponding remainders are different, i.e., $ak \not\equiv ak' \pmod p$. This is equivalent to $a(k - k') \not\equiv 0 \pmod p$.

By hypothesis $p \nmid a$ and, in addition, $p \nmid (k - k')$ because $-p < k - k' < p$. Using again the converse of the statement of Problem 4(x), we obtain that $p \nmid a(k - k')$ and thus $\mathcal{A} = \{1, \ldots, p-1\}$.

(iii) By the properties of modular arithmetic, we have the following sequence of equivalences modulo p:

$$(p-1)!a^{p-1} \equiv \prod_{k=1}^{p-1} ka \equiv \prod_{k=1}^{p-1} (ka \mathbf{\ mod\ } p) \equiv \prod_{x \in \mathcal{A}} x \equiv (p-1)! \pmod p,$$

where the third equivalence follows from point (ii).

Thus, we showed that for any a coprime with p, we have

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod p.$$

Therefore, $p \mid (p-1)!(a^{p-1} - 1)$. Since p is prime and cannot divide any $k < p$, again using the statement of Problem 4(x), we obtain that $p \mid (a^{p-1} - 1)$, which implies that $p \mid a(a^{p-1} - 1)$. This last expression is equivalent to $a^p \equiv a \pmod p$.