Discrete Structures EPFL, Fall 2013

Graded Problem Set 6

Date: 25.10.2013 Due date: 1.11.2013, noon

Instructions: Please write the solution for each problem on a separate piece of paper. Sort these pieces of paper, with Problem 1 on top. Add this page as cover page, fill in your name, Sciper number, and the list of collaborators, and staple them all together on the left top.

Rules: You are allowed and encouraged to discuss these problems with your colleagues. However, each of you has to write down her solution in her own words. If you collaborated on a homework, write down the name of your collaborators and your sources in the space below. No points will be deducted for collaborations. But if we find similarities in solutions beyond the listed collaborations we will consider it as cheating. Please note that EPFL has a VERY strict policy on cheating and you might be in BIG trouble. It is simply not worth it.

Grading: Each problem is worth 20 points.

Collaborators and sources:

First name: .....

Last name: .....

Sciper: .....

Problem 1 ... / 20

Problem 2 ... / 20

Problem 3 ... / 20

Problem 4 ... / 20

Problem 5 ... / 20

TOTAL ... / 100

Problem 1. Let f be an arbitrary function from $\mathbb{N}$ to $\mathbb{R}^+$.

(a) Let g_1, g_2 be two functions from $\mathbb{N}$ to $\mathbb{R}^+$ such that g_1 and g_2 are both $\Theta(f)$. Show that the function $g_1 + g_2$ is $\Theta(f)$ or provide a counterexample.

(b) With g_1,g_2 as above, show that the function $g_1 g_2$ is $\Theta(f^2)$ or provide a counterexample.

(c) Let g_3, g_4 be two functions from $\mathbb{N}$ to $\mathbb{R}$ such that g_3 and g_4 are both $\Theta(f)$. Show that the function $g_3 + g_4$ is $\Theta(f)$ or provide a counterexample.

(d) With g_3, g_4 as above, show that the function $g_3 g_4$ is $\Theta(f^2)$ or provide a counterexample.

Problem 2.

(a) Determine whether there exists a function $f : \mathbb{N} \to \mathbb{R}^+$ such that

(i) f is NOT $\Omega(n)$;

(ii) f is NOT $o(e^n)$.

If such a function exists, write one possible f.

(b) Let $g(n) = (\lceil \log_2 n \rceil)!$. Show that

(i) $g(n) = \Omega(n^{2013})$;

(ii) $g(n) = o(2^n)$.

Problem 3. Find a set $\mathcal{C}$ of functions from $\mathbb{N}$ to $\mathbb{R}^+$ such that the following three conditions are fulfilled (at the same time!).

(i) For any $f \in \mathcal{C}$, $f = o(n \cdot (\log n)^{47})$ and $f = \Omega(n \cdot (\log n)^{46})$.

(ii) For any $f_1, f_2 \in \mathcal{C}, f_1 \neq f_2$, either $f_1 = o(f_2)$ or $f_2 = o(f_1)$.

(iii) The set $\mathcal{C}$ has the cardinality of the continuum (i.e. $|\mathcal{C}| = |\mathbb{R}|$).

Problem 4. Prove or disprove the following statements.

(i) For all integers a, b, c, d, if $a \mid b$ and $c \mid d$, then $(a + c) \mid (b + d)$.

(ii) For all integers a, b, c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

(iii) For all integers a, b, c, if $a \mid c$ and $b \mid c$, then $(a + b) \mid c$.

(iv) For all integers a, b, c, d, if $a \mid b$ and $c \mid d$, then $(ac) \mid (b + d)$.

(v) For all positive integers a, b, if $a \mid b$ and $b \mid a$, than $a = b$.

(vi) For all integers a, b, if $a \mid b$ and $b \mid a$, then $a = b$.

(vii) For all integers a, b, c, if $a \mid (b + c)$, then $a \mid b$ and $a \mid c$.

(viii) For all integers a, b, c, if $a \mid bc$, then $a \mid b$ or $a \mid c$.

(ix) For all integers a, b, c, if $a \mid c$ and $b \mid c$, then $ab \mid c^2$.

(x) For all positive primes a and all positive integers b and c, if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Problem 5. The goal of this exercise is to prove *Fermat's little theorem*, which states that for any prime p and any natural number a,

$$a^p \equiv a \pmod{p}.$$

(i) Suppose that $\gcd(a, p) \neq 1$. Then, prove the claim, which in this case becomes trivial.

(ii) Suppose that $\gcd(a, p) = 1$. Let $\mathcal{A}$ be the set of the remainders of the division of $k \cdot a$ by p for $k = 1, \ldots, p-1$, i.e., $\mathcal{A} = \{ka \textbf{ mod } p : k \in \{1, \ldots, p-1\}$. Prove that $\mathcal{A} = \{1, \ldots, p-1\}$.

(iii) Compute $\prod_{k=1}^{p-1} ka$ and use point (ii) to prove the theorem when $\gcd(a, p) = 1$.