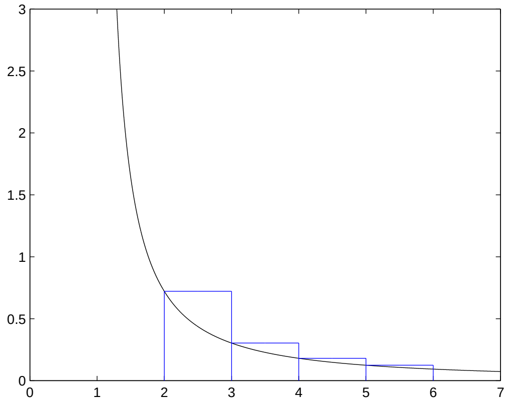
Solution to Graded Problem Set 6

Date: 24.10.2013 Due date: 31.10.2013

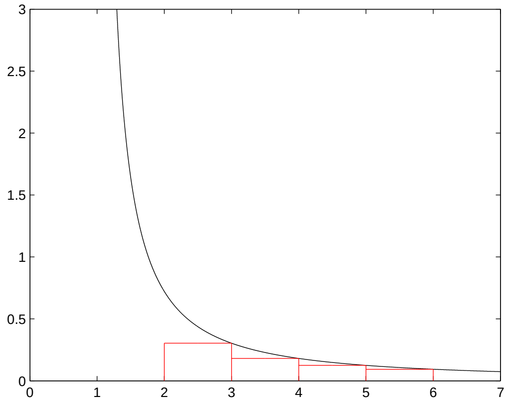
Problem 1. By using the same technique seen in class to bound $n!$, we have that

$$\sum_{i=2}^{n} \frac{1}{i\log i} - \frac{1}{2\log 2} = \sum_{i=3}^{n} \frac{1}{i\log i} \leq \int_{2}^{n} \frac{1}{x\log x}dx \leq \sum_{i=2}^{n-1} \frac{1}{i\log i} \leq \sum_{i=2}^{n} \frac{1}{i\log i}.$$

The upper and lower bounds are represented in the Figure below.



(a) Upper bound



(b) Lower bound

Figure 1: The black curve is the function $f(x) = \frac{1}{x\log x}$, the blue rectangles are an upper bound and the red rectangles are a lower bound.

A simple calculation shows that

$$\int_2^n \frac{1}{x \log x} dx = \log\log n - \log\log 2.$$

Hence,

$$\log\log n - \log\log 2 \leq \sum_{i=2}^{n} \frac{1}{i \log i} \leq \log\log n - \log\log 2 + \frac{1}{2\log 2}. \tag{1}$$

Note that $\log\log 2 < 0$. Then, $\log\log n - \log\log 2 \geq \log\log n$, and, therefore, the lower bound in (1) gives that $\sum_{i=2}^{n} \frac{1}{i \log i}$ is $\Omega(\log\log n)$ (one suitable choice of the witnesses is $C = 1$ and $k = 2$). As $-\log\log 2 + \frac{1}{2\log 2} < 2$ and $\log\log n > 2$ for $n > e^{e^2}$, the upper bound in (1) gives that $\sum_{i=2}^{n} \frac{1}{i \log i}$ is $O(\log\log n)$ (one suitable choice of the witnesses is $C = 2$ and $k = e^{e^2}$). Therefore, $\sum_{i=2}^{n} \frac{1}{i \log i}$ is $\Theta(\log\log n)$.

Problem 2.

a) For any f and g which attain only positive values, we have that

$$\frac{f(n) + g(n)}{2} \leq \max\{f(n), g(n)\} \leq f(n) + g(n) \qquad \forall n \in \mathbb{N}.$$

The lower bound allows us to prove that $\max\{f(n), g(n)\}$ is $\Omega(f(n) + g(n))$ (one suitable choice of the witnesses is $C = 1/2$ and $k = 0$). The upper bound allows us to prove that $\max\{f(n), g(n)\}$ is $O(f(n) + g(n))$ (one suitable choice of the witnesses is $C = 1$ and $k = 0$).

b) The statement is false. For example, take $f(n) = n + 1$ and $g(n) = 1$. Then,

$$\min\{f(n), g(n)\} = 1 \qquad \forall n \geq 0.$$

Clearly, $n + 2$ is not $\Theta(1)$, because $n + 2$ is not $O(1)$.

Problem 3.

a) **True.** Indeed, $2^{n+1} = 2 \cdot 2^n$. Hence, if we take $C = 2$ and $k = 0$, we have that $2^{n+1} \leq C2^n$ for any $n \geq k$. By definition, this implies the desired result.

b) **False.** Note that

$$\frac{2^{2n}}{2^n} = 2^n.$$

Suppose that there exist C and k s.t. $2^{2n} \leq C2^n$ for any $n \geq k$. Then, $2^n \leq C$, but eventually 2^n goes to $+\infty$, which means that we cannot find such C. As a result, 2^{2n} is not $O(2^n)$.

c) **False.** Pick $f(x) = 2x$, $g(x) = x$, and $h(x) = 2^x$. Then, clearly $f(n)$ is $O(g(n))$, but, according to the previous point, $h(f(x))$ is not $O(h(g(x)))$.

Problem 4.

a) **False.** 3 is prime, 5 is prime, but $3 + 5$ is not prime.

b) **False.** $-\sqrt{2}$ and $\sqrt{2}$ are irrational numbers, but $-\sqrt{2} + \sqrt{2} = 0$, which is a rational number.

c) **False.** $1/2$ is a non-zero rational number, but $(1/2)^{1/2} = \sqrt{2}/2$ is irrational.

d) **False.** $f(17) = 17^2$ is not prime.

e) **True.** Both p and q are odd. Hence, $pq+1$ is an even number, which implies that it cannot be prime.

Problem 5.

a) $7 \times 8 = 56 \equiv 1 \pmod{11}$. Hence the multiplicative inverse of 7 modulo 11 is 8.

b) Does not exist. The multiplicative inverse of a modulo m exists if and only if a and m are coprime (i.e. if $\gcd(a,m) = 1$) but $\gcd(6,8) = 2$.

c) $5 \times 5 = 25 \equiv 1 \pmod 8$. Hence the multiplicative inverse of 5 modulo 8 is 5 itself (note that in this case since 5 and 8 are coprime the multiplicative inverse exists).

d) We want to find m such that $6^m \mid 73!$ but $6^{m+1} \nmid 73!$. Suppose the prime factorization of 73! is $73! = 2^\alpha \times 3^\beta \times$ other prime factors. Since $6^m = 2^m \times 3^m$ 6^m divides 73! if and only if $m \leq \min\{\alpha, \beta\}$. So, by setting $m = \min\{\alpha, \beta\}$, $6^m \mid 73!$ but $6^{m+1} \nmid 73!$.

   We first compute β: There are $\lfloor \frac{73}{3} \rfloor = 24$ multiples of 3, $\lfloor \frac{73}{9} \rfloor = 8$ multiples of 9 and $\lfloor \frac{73}{27} \rfloor = 2$ multiples of 27 in $\{1, 2, \ldots, 73\}$. Thus $\beta = 24 + 8 + 2 = 34$.

   Now, it is easy to see that $\alpha \geq \beta$ since there are at least 36 even numbers in $\{1, 2, \ldots, 73\}$. Thus, $\min\{\alpha, \beta\} = 34$.

   Therefore, the answer to the question is $m = 34$. $6^{34} \mid 73!$ but $6^{35} \nmid 73!$.

e) Since 17 and $9 \nmid 17$, $9^{17-1} = 9^{16} \equiv 1 \pmod{17}$. Since $123456789 \equiv 5 \pmod{16}$,

$$9^{123456789} = 9^{16} \times 9^{16} \times \cdots \times 9^{16} \times 9^5 \equiv 9^5 \pmod{17}$$

   thus

$$9^{123456789} \equiv 9^5 \equiv 8 \pmod{17}.$$

Problem 6. The proof is by contradiction. Suppose that there exists only a finite number of primes. Let's say that there are K primes, namely $p_1 < p_2 < \cdots < p_K$. Consider the number

$$\bar{n} = \prod_i^K p_i + 1.$$

The remainder of the division of $\bar{n}$ by p_i is 1 for any $i \in \{1, \cdots, K\}$. Hence, $p_i \nmid \bar{n}$. This implies that $\bar{n}$ is coprime with p_i for any $i \in \{1, \cdots, K\}$.

By assumption, $p_1, p_2, \cdots, p_K$ are all the prime numbers. Therefore, $\bar{n}$ is coprime with all the prime numbers, which means that it is a prime number itself. As a result, we have found another prime number different from $p_1, p_2, \cdots, p_K$. This is a contradiction.

Note that, in general, if you take the product of some primes and you add 1, you will not necessarily obtain a prime number. Indeed, the result is only coprime with the prime numbers that you choose to multiply!