Discrete Structures EPFL, Fall 2014

Problem Set 7

Date: 31.10.2013 Not graded

Problem 1. In the last exercise session you were asked some questions about multiplicative inverses and (most likely ☺) you solved them by trial and error. However, this week you have learned in class more powerful techniques that allow you to solve this kind of problems systematically!

a) Let us start from the exercises in Problem Set 6. You were asked to find the multiplicative inverse of 7 modulo 11, the multiplicative inverse of 6 modulo 8, and the multiplicative inverse of 5 modulo 8. In which cases such a multiplicative inverse did actually exist?

b) Pick $a, b \in \mathbb{N}$. Find a necessary and sufficient condition for the existence of the multiplicative inverse of a modulo b. Then, find a necessary and sufficient condition also for the existence of the multiplicative inverse of b modulo a. Check that these conditions are consistent with the result of point a).

c) Pick $a, b \in \mathbb{N}$ s.t. the multiplicative inverse of a modulo b exists. Describe an algorithm that finds it.

d) Apply the algorithm of point c) to find

   i. the multiplicative inverse of 57 modulo 148.
   ii. the multiplicative inverse of 123 modulo 341.
   iii. the multiplicative inverse of 257 modulo 921.

Problem 2. In this problem we will show, by steps, that $\sum_{\substack{p\geq 1 \\ p \text{ prime}}} \frac{1}{p}$ is $\Omega(\log \log n)$. Let p_k be the k^{th} largest prime, and let the set $\mathcal{A}_n$ be defined by

$$\mathcal{A}_n = \{p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n} : 0 \leq i_1, i_2, \ldots, i_n \leq n\}.$$

It is very important that you work the details of each step!

a) Convince yourself, using the unique factorization theorem, that

$$\left(1 + \frac{1}{p_1} + \ldots + \frac{1}{p_1^n}\right)\left(1 + \frac{1}{p_2} + \ldots + \frac{1}{p_2^n}\right) \ldots \left(1 + \frac{1}{p_n} + \ldots + \frac{1}{p_n^n}\right) = \sum_{m \in \mathcal{A}_n} \frac{1}{m}. \quad (1)$$

b) Use the sum of the geometric series to show that the left hand side of the equation above is upper bounded by

$$\left(1 + \frac{1}{p_1 - 1}\right)\left(1 + \frac{1}{p_2 - 1}\right) \ldots \left(1 + \frac{1}{p_n - 1}\right).$$

c) Take the natural logarithm on both sides of (1) and, using b), show that

$$\sum_{j=1}^{n} \frac{1}{p_j - 1} \geq \ln \sum_{m \in \mathcal{A}_n} \frac{1}{m}.$$

d) After proving that $\{1, \ldots, n\} \subseteq \mathcal{A}_n$, use it to show that

$$1 + \sum_{j=1}^{n-1} \frac{1}{p_j} \geq \ln \sum_{m=1}^{n} \frac{1}{m}. \tag{2}$$

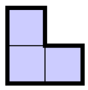
e) Conclude, using an estimate on the growth rate of $\sum_{m=1}^{n} \frac{1}{m}$ proved in class, that $\sum_{j=1}^{n} \frac{1}{p_j}$ is $\Omega(\log \log n)$.

Problem 3. Use mathematical induction (in its original or strong form) to show the following:

a) $2^{2n} - 1$ is divisible by 3 for any integer $n \geq 1$.

b) Let $a, b \in \mathbb{N}$. Then, $a^n - b^n$ is divisible by $a - b$ for any integer $n \geq 1$.

Problem 4. Consider a $2^n \times 2^n$ grid of 2^{2n} squares arranged in 2^n rows and 2^n columns. If we remove one square from this grid of 2^{2n} squares, we obtain a shape. Let $\mathcal{C}_n$ be the set of shapes obtained by removing one square from the grid of 2^{2n} squares. We also say that a shape is *cool* if it can be tiled, namely, completely covered without overlapping, with L-shaped tiles occupying exactly 3 squares, like this:



Prove that, for any integer $n \geq 1$, any shape in $\mathcal{C}_n$ is *cool*.

Problem 5. Consider the following theorem.

Theorem. Every integer > 1 has a unique prime factorization.

The result is true (as you have seen in class), but the following "proof" by induction is not correct. Where is the flaw?

Proof. By strong induction. Let $P(n)$ be the statement that n has a unique factorization. We prove $P(n)$ for any $n > 1$.

Base step, $n = 2$. $P(2)$ is clearly true.

Induction step: Assume $P(2), \cdots, P(n)$. We want to prove $P(n+1)$.

If $n+1$ is prime, then we are done. If not, it factors somehow. Suppose $n+1 = r \cdot s$ for some $r, s > 1$. By the induction hypothesis, r has a unique factorization $\prod_i p_i$ and s has a unique prime factorization $\prod_j q_j$. Thus, $\prod_i p_i \prod_j q_j$ is a prime factorization of $n+1$. In addition, since the factorization of both r and s is unique, also the factorization of $n+1$ must be unique. $\square$