**Homework #8. Due on Friday, March 30th by 1pm in TA's mailbox**

**Reading:**

1. For this assignment: sections 4.3, 5.1 and beginning of 5.2 of the BOOK (throughout this assignment BOOK refers to the book 'A discrete transition to advanced mathematics') and class notes from Lectures 15-16.
2. For next week's classes: sections 5.2 and 6.1.

**Practice problems from the BOOK:** From 5.1: 3, 5, 7, 11(b)(i)(iii)(v); from 5.2: 1, 3, 8.

**Problems to hand in:**

**0.** Redo problems 2,3,4 and 5 from HW#6 (can be resubmitted for 90% credit); see some comments on these problems at the end of the assignment.

**1.** Let $N$ denote the number of passwords consisting of 6 lowercase English letters in which the letter 'a' appears at least once.

(a) Use the inclusion-exclusion principle to prove that

$$N = 6 \cdot 26^5 - \binom{6}{2} \cdot 26^4 + \binom{6}{3} \cdot 26^3 - \binom{6}{4} \cdot 26^2 + \binom{6}{5} \cdot 26 - 1.$$

Recall that we gave an outline of this proof in Lecture 15.

(b) In Lecture 15 we proved that $N = 26^6 - 25^6$ using a different counting argument. Use the binomial theorem to show directly that the two expressions for $N$ are equal to each other.

**2.** Given $n \in \mathbb{N}$, define $RP(n)$ to be the set of all integers between 1 and $n$ which are relatively prime to $n$, and let $\phi(n) = |RP(n)|$. For instance, $RP(2) = \{1\}$, so $\phi(2) = 1$; $RP(3) = \{1, 2\}$, so $\phi(3) = 2$; $RP(4) = \{1, 3\}$, so $\phi(4) = 2$; $RP(5) = \{1, 2, 3, 4\}$, so $\phi(5) = 4$; $RP(6) = \{1, 5\}$, so $\phi(6) = 2$ etc. The obtained function $\phi : \mathbb{N} \to \mathbb{N}$ is called the *Euler function*.

The goal of this problem is to use the inclusion-exclusion principle to prove the following formula for the Euler function: If $n = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct primes and each $a_i \in \mathbb{N}$ (here it is essential that each $a_i$ is positive), then

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) \qquad (***)$$

Note that since $(1 - \frac{1}{p_i}) = \frac{p_i - 1}{p_i}$, the above formula can be rewritten as $\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.

So assume that $n = p_1^{a_1} \dots p_k^{a_k}$ with $p_i$ and $a_i$ as above. For each $1 \leq i \leq k$ let $A_i$ be the set of all integers from 1 to $n$ divisible by $p_i$, and let $A = \cup_{i=1}^k A_i$

(a) Prove that $\phi(n) = n - |A|$.

(b) Prove that $|A_i| = \frac{n}{p_i}$ for each $i$, $|A_i \cap A_j| = \frac{n}{p_i p_j}$ if $i$ and $j$ are distinct etc.

(c) Now use (a), (b) and the inclusion-exclusion principle to prove the formula (***). It may be easier to expand the product in (***) and show that the obtained expansion is equal to the right-hand side of the formula in the inclusion-exclusion principle.

**3.** Problem 2 from Section 5.1 (make sure to prove your answer)

**4.** Problem 4 from Section 5.1 (make sure to prove your answer)

**5.** Problem 8 from Section 5.1 (the definition of the domain and range of a relation appear on page 165)

**6.** Consider the relation $R$ on $\mathbb{Z}$ given by $xRy \iff x + y$ is even. Prove that $R$ is an equivalence relation. Recall that we already checked symmetry and reflexivity in class, so you only need to prove transitivity.

**Some comments of problems 2-5 from HW#4.**

**Problem 2.** Make sure you are proving exactly what you are asked to: if $n = \prod_{i=1}^k p_i^{a_i}$ where $p_1, \dots, p_k$ are distinct prime and each $a_i \in \mathbb{N}$ and if $n = m^2$ for some $m \in \mathbb{N}$, then each $a_i$ is even.

**Problem 4.** Recall that we discussed how to start on this problem in Lecture 16.

**Problem 5.** Here is a completely formal definition of the $ord_p$ function (which may be helpful for writing a formal argument). Let $n \in \mathbb{N}$, and write $n = \prod_{i=1}^k p_i^{a_i}$ where $p_1, \dots, p_k$ are distinct primes and each $a_i \in \mathbb{Z}_{\geq 0}$. If $p$ is any prime, define

$$ord_p(n) = \begin{cases} a_i & \text{if } p = p_i \text{ for some } 1 \leq i \leq k \\ 0 & \text{if } p \notin \{p_1, \dots, p_k\} \end{cases}$$

Note that it is Ok to allow some $a_i$ equal to 0 here – for instance, we can write 45 as $3^2 \cdot 5^1$ or, say, as $3^2 \cdot 5^1 \cdot 7^0$. The definition of $ord_p(45)$ does not depend on which of these factorizations we use.

**General suggestion:** It may be more convenient to solve these problems in a different order: 5,3,2,4 since one can use 5(a) to solve 3 and 3 and/or 5(a) to solve 2.