Solutions to Homework #8.

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.

Solution: (a) For each $1 \le i \le 6$ let A_i denote the set of passwords whose i^{th} letter is a. Then $\cup_{i=1}^6 A_i$ is precisely the set of passwords which have at least one a. By the inclusion-exclusion principle we have

$$|\cup_{i=1}^6 A_i| = \sum_{i=1}^6 |A_i| - \sum_{1\le i<j\le 6} |A_i \cap A_j| + \sum_{1\le i<j<k\le 6} |A_i \cap A_j \cap A_k| - \ldots \quad (***)$$

For each $1 \le i \le 6$ we have $|A_i| = 26^5$. Indeed, if we want to construct a password which lies in A_i, we have one choice for the i^{th} letter (which has to be a) and 26 choices for each of the remaining 5 letters. Thus, $|A_i| = 26^5$ for each i and $\sum_{i=1}^6 |A_i| = 6 \cdot 26^5$.

Now suppose $1 \le i < j \le 6$. If we want to construct a password in $A_i \cap A_j$ we have one choice for the i^{th} and j^{th} letters and 26 choices for each of the remaining 4 letters, so $|A_i \cap A_j| = 26^4$. Since there are $\binom{6}{2}$ ways to choose a pair (i, j) with $1 \le i < j \le 6$, we get $\sum\limits_{1\le i<j\le 6} |A_i \cap A_j| = \binom{6}{2} \cdot 26^4$. Similarly, $\sum\limits_{1\le i<j<k\le 6} |A_i \cap A_j \cap A_k| = \binom{6}{3} \cdot 26^3$ etc. Plugging in the obtained expressions for $\sum_{i=1}^6 |A_i|$, $\sum\limits_{1\le i<j\le 6} |A_i \cap A_j|$ etc. into (***), we obtain the desired formula for N.

(b) To see that $N = 26^6 - 25^6$ we just need to write 25^6 as $(26 + (-1))^6$ and use the binomial theorem.

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 $\phi(n) = \prod\limits_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.

So assume that $n = p_1^{a_1} \dots p_k^{a_k}$ with p_i and a_i as above. For each $1 \le i \le k$ 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.

Solution: (a) As usual let $[n] = \{1, \dots, n\}$. We claim that $RP(n)$ is precisely the complement of A in $[n]$ (if this is proved, it follows that $\phi(n) = |RP(n)| = |[n]| - |A| = n - |A|$).

By definition, $A = \cup_{i=1}^{k} A_i$ is the set of elements of $[n]$ which are divisible by p_i for at least one i. Hence A^c, the complement A, is the set of elements of $[n]$ which are not divisible by any of p_i's; in other words, A^c is the set of elements of $[n]$ whose prime factorization does not involve any of p_i's. Equivalently, A^c is the set of elements of $[n]$ which do not have any common prime factors with n. By HW#6.5(c) this set is precisely the set of elements of $[n]$ which are relatively prime to n, that is, $A^c = RP(n)$.

(b) Integers divisible by p_i are precisely integers of the form kp_i with $k \in \mathbb{Z}$. We need to count how many values of k satisfy the condition $kp_i \in [n]$. Given $k \in \mathbb{Z}$, we have $kp_i \in [n] \iff 1 \le kp_i \le n \iff \frac{1}{p_i} \le k \le \frac{n}{p_i} \iff 1 \le k \le \frac{n}{p_i}$. Since $\frac{n}{p_i} \in \mathbb{N}$, we have $\frac{n}{p_i}$ choices for k such that $kp_i \in [n]$, so $|A_i| = \frac{n}{p_i}$.

Now take any $i < j$. By definition the set $A_i \cap A_j$ consists of integers in $[n]$ which are divisible by p_i and by p_j. Since p_i and p_j are distinct primes, FTA easily implies that being divisible by p_i and p_j is the same as being divisible by $p_i p_j$. Thus, $|A_i \cap A_j|$ is the number of integers in $[n]$ divisible by

$p_i p_j$. This number is equal to $\frac{n}{p_i p_j}$ by the same argument as in the previous paragraph.

(c) Combining (a),(b) and the inclusion-exclusion principle, we conclude that

$$|RP(n)| = n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{1 \le i < j \le k} \frac{n}{p_i p_j} - \ldots = n(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{1 \le i < j \le k} \frac{1}{p_i p_j} - \ldots)$$

Thus, we just need to prove that the last expression equals $n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$.

We argue similarly to the combinatorial proof of the binomial theorem. Indeed, $\prod_{i=1}^{k}(1 - \frac{1}{p_i}) = ((1 + (-\frac{1}{p_1}))(1 + (-\frac{1}{p_2})) \ldots (1 + (-\frac{1}{p_k}))$. When we expand this product, we get a sum of terms of the form $x_1 \ldots x_k$, where $x_i = 1$ or $x_i = -\frac{1}{p_i}$ for each i. For each such product $X = x_1 \ldots x_k$ let $S(X) = \{i \mid x_i = -\frac{1}{p_i}\}$. Then $X = \frac{(-1)^{|S(X)|}}{\prod_{i \in S} p_i}$ if $S(X) \neq \emptyset$ and $X = 1$ if $S(X) = \emptyset$. In general, $S(X)$ could be any subset $\{1, \ldots, k\}$ (we have exactly one term for each subset). By the above computations, the sum of all such products with $|S(X)| = 1$ is $\sum\limits_{i=1}^{k} \frac{(-1)^1}{p_i} = -\sum\limits_{i=1}^{k} \frac{1}{p_i}$; the sum of all such products with $|S(X)| = 2$ is $\sum\limits_{1 \le i < j \le k} \frac{(-1)^2}{p_i p_j} = \sum_{i=1}^{k} \frac{1}{p_i p_j}$ etc. Hence the sum of all products (including the one with $S(X) = \emptyset$) is equal to

$$1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{1 \le i < j \le k} \frac{1}{p_i p_j} - \ldots,$$

as desired.

3. Problem 2 from Section 5.1.

Solution: By definition, relations from A to B are subsets of $A \times B$. We know that a set with k elements has precisely 2^k subsets. Since $|A \times B| = |A| \cdot |B| = nm$, we conclude that there are 2^{nm} subsets of $A \times B$ and hence 2^{nm} relations from A to B.

4. Problem 4 from Section 5.1.

Solution: (a) If R is a relation on A which is both antisymmetric and symmetric, then R cannot contain elements of the form (a, b) with $b \neq a$. Indeed, if $(a, b) \in R$ and R is symmetric, then $(b, a) \in R$. If we also have $b \neq a$, this contradicts the assumption that R is antisymmetric.

Thus, if R is both symmetric and antisymmetric, then every element of R must be equal to (a, a) for some $a \in A$. Conversely, it is clear from definitions that any relation which only contains elements of the form (a, a) is both symmetric and antisymmetric.

(b) The only such relation is the identity relation $\mathrm{id}_A = \{(a,a) \mid a \in A\}$. Indeed, a reformulation of our answer in (a) is that if R is antisymmetric and symmetric, then $R \subseteq \mathrm{id}_A$. On the other hand, R is reflexive (again by a reformulation of the definition) $\iff R \supseteq \mathrm{id}_A$. Thus, R is antisymmetric, symmetric and reflexive $\iff$ ($R \subseteq \mathrm{id}_A$ and $R \supseteq \mathrm{id}_A$) $\iff R = \mathrm{id}_A$.

5. Problem 8 from Section 5.1.

Solution: Since $domain(R) = \{1,2,3\}$, R must contain at least one element of the form $(1,a)$, at least one element of the form $(2,b)$ and at least one element of the form $(3,c)$. Since $|R| = 3$ and we already listed 3 required elements (which are clearly distinct), R cannot contain any other elements. Finally, since $range(R) = \{1,2,3\}$, the numbers a, b and c above must be distinct.

Thus, we have $6 = 3!$ relations with the required property:
$R_1 = \{(1,1),(2,2),(3,3)\}$, $R_2 = \{(1,1),(2,3),(3,2)\}$, $R_3 = \{(1,2),(2,1),(3,3)\}$, $R_4 = \{(1,2),(2,3),(3,1)\}$, $R_5 = \{(1,3),(2,1),(3,2)\}$, $R_6 = \{(1,3),(2,2),(3,1)\}$.
The table listing the required properties is given below:

relation	reflexive	transitive	symmetric	antisymmetric
R_1	Y	Y	Y	Y
R_2	N	N	Y	N
R_3	N	N	Y	N
R_4	N	Y	N	Y
R_5	N	Y	N	Y
R_6	N	N	Y	N

6. Consider the relation R on $\mathbb{Z}$ given by $xRy \iff x+y$ is even. Prove that R is an equivalence relation.

Note: Below we will also describe the equivalence classes with respect to R (this was not part of the homework problem).

First solution. First we prove that R is an equivalence relation:

Reflexivity: For any x we have $2 \mid 2x^2$, so $2 \mid (x^2 + x^2)$, whence xRx.

Symmetry: $2 \mid (x^2 + y^2)$ if and only if $2 \mid (y^2 + x^2)$ by commutativity of addition.

Transitivity: Suppose that $2 \mid (x^2+y^2)$ and $2 \mid (y^2+z^2)$. Then $x^2+y^2 = 2k$ and $y^2+z^2 = 2m$ for some $k, m \in \mathbb{Z}$. Therefore, $x^2 = 2k-y^2$, $z^2 = 2m-y^2$, and we get $x^2+z^2 = 2(k+m-y^2)$, so $2 \mid (x^2+z^2)$.

To describe the equivalence classes we start with some elements of $\mathbb{Z}$, say, 0, and find all elements in its equivalence class – we get

$$[0] = \{x \in \mathbb{Z} : x^2 + 0^2 \text{ is even }\} = \{x \in \mathbb{Z} : x \text{ is even }\} = \{2k \mid k \in \mathbb{Z}\}.$$

Then take any element outside of [0], say, 1, and compute its equivalence class; we get

$$[1] = \{x \in \mathbb{Z} : x^2 + 1^2 \text{ is even }\} = \{x \in \mathbb{Z} : x \text{ is odd }\} = \{2k+1 \mid k \in \mathbb{Z}\}.$$

Since the union of [0] and [1] is the set of all integers, we found that there are two equivalence classes:

$$[0] = \{2k : k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \ldots\} \text{ and } [1] = \{2k+1 : k \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \pm 7, \ldots\}.$$

Second (shorter) solution. This solution is based on the following observation:

$$xRy \iff x \text{ and } y \text{ are both even or both odd. (***)}$$

From (***) it is clear that R is reflexive and symmetric. Now we prove transitivity: Assume xRy and yRz.

Case 1: y is even. Then x is even since xRy, and z is even since yRz, so both x and z are even, whence xRz.

Case 2: y is odd. By analogous argument, x and z are both odd, so xRz.

Thus in either case, xRz holds, which proves transitivity.

Finally, the description of equivalence classes obtained in the first solution follows immediately from (***).