Sample: Combinatorics Number Theory - The Inclusion-Exclusion Principle

Task 1.

Let n be a positive integer and $p_1, \dots, p_k$ be all the different prime numbers that divide n. Consider the Euler function ϕ defined by

$$\phi(n) = \big|\{k \ : \ 1 \leq k, \ GCD\{k, n\} = 1\}\big|.$$

Use the inclusion-exclusion principle to show that

$$\phi(n) = n \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}).$$

Proof. The number n has the following form:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k},$$

where $p_1, \dots, p_k$ are mutually distinct prime numbers, and $a_i \geq 1$.

We will use induction on k.

1) Suppose $k = 1$, so $n = p^a$, where p is a prime number and $a \geq 1$. Then formula

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

reduces to

$$\phi(n) = \phi(p^a) = p^a(1 - \tfrac{1}{p}) = p^a - p^a \cdot \frac{1}{p} = p^a - p^{a-1}.$$

Let $A = \{1, \dots, p^a\}$, and B be the subset consisting of all numbers k that are not relatively prime with $n = p^a$, that is

$$B = \{k \mid 1 \leq k \leq p^a, GCD\{k, n\} \neq 1\}.$$

Hence

$$A \setminus B = \{k \mid 1 \leq k \leq p^a, GCD\{k, n\} = 1\},$$

and so, by definition of the function ϕ we have that

$$\phi(n) = |A \setminus B|.$$

Thus we should to prove that

$$|A \setminus B| = p^a - p^{a-1}.$$

Notice that $GCD(k, p^a) \neq 1$, i.e. $k \in B$, if and only if $GCD(k, p) \neq 1$ that is k is divided by p.

Let $C = \{1, 2, \dots, p^{a-1}\}$. We claim that $k \in B$ if and only if $k = pm$, where $m \in C$.

Indeed, if $k \in B$, so k is divided by p, then $k = pm$ for some m. Since $k = pm \leq p^a$, it follows that $m \leq p^{a-1}$, that is $m \in C$.

Conversely, if $m \in C$, then $k = pm \in B$. This implies that $|B| = |C| = p^{a-1}$. Since $|A| = p^a$, we obtain that

$$|A \setminus B| = |A| - |B| = p^a - p^{a-1}.$$

2) Suppose we have proved formula

$$\phi(n) = n \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}).$$

for some k. Let us prove it for $k + 1$.

Thus assume that

$$n = xp^a,$$

where $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, p is a prime number distinct from $p_1 \ldots, p_k$, and

$$\phi(x) = x \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}).$$

We should prove that

$$\phi(n) = n(1 - \tfrac{1}{p}) \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}) = xp^a(1 - \tfrac{1}{p}) \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}) =$$

$$= x \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}) \cdot p^a(1 - \tfrac{1}{p}) = \phi(x)(p^a - p^{a-1}).$$

Let $A = \{0, \ldots, xp^a - 1\}$, and $B \subset A$ be the subset consisting of all numbers that are not relatively prime with xp^a. Notice that $GCD(k, xp^a) \neq 1$ if and only if either $GCD(k, x) \neq 1$ or $GCD(k, p) \neq 1$.

Let also $X \subset A$ be the subset consisting of all numbers that are not relatively prime with x, and $P \subset A$ be the subset consisting of all numbers that are not relatively prime with P.

Then $A \setminus (X \cup P)$ is the set of all $k \in A$ which are relatively prime with $n = xp^a$

$$|A \setminus (X \cup P)| = \{k \ : \ 1 \leq k \leq n, \ GCD(k, n) = 1\},$$

so, by definition of the function ϕ we have that

$$\phi(n) = |A \setminus (X \cup P)|.$$

Thus we need to prove that

$$|A \setminus (X \cup P)| = \phi(x)(p^a - p^{a-1}).$$

Notice that

$$|A \setminus (X \cup P)| = |A| - |X| - |P| + |X \cap P|.$$

We have that

$$|A| = n = xp^a.$$

Let us compute $|X|$. Notice that every $k \in A$ can be uniquely written in the following form:

$$k = \alpha x + \beta,$$

where $\alpha \in \{0, 1, \ldots, p^a - 1\}$ and $\beta \in \{0, \ldots, x-1\}$. Moreover, $GCD(k, x) \neq 1$, i.e. $k \in X$ if and only if $GCD(\beta, x) \neq 1$. But for such β we have $x - \phi(x)$ possibilities. Therefore

$$|X| = \big|\{0, 1, \ldots, p^a - 1\}\big| \cdot (x - \phi(x)) = p^a(x - \phi(x)).$$

Similarly, every $k \in A$ can be uniquely written in the following form:

$$k = \gamma p^a + \delta,$$

where $\gamma \in \{0, 1, \ldots, x-1\}$ and $\delta \in \{0, \ldots, p^a - 1\}$. Moreover, $GCD(k, p^a) \neq 1$, i.e. $k \in P$ if and only if $GCD(\delta, p^a) \neq 1$. But for such β we have $p^a - \phi(p^a) = p^{a-1}$ possibilities. Therefore

$$|P| = \big|\{0, 1, \ldots, x - 1\}\big| \cdot p^{a-1} = xp^{a-1}.$$

Finally, suppose $k \in X \cap P$, so $GCD(k, p) \neq 1$ and $GCD(k, x) \neq 1$. Thus $k = mp$ for some $m \in \{0, \ldots, xp^{a-1}\}$, and $GCD(m, x) \neq 1$ since $GCD(x, p) = 1$. Then similarly to computations of $|X|$ we have that

$$|X \cap P| = p^{a-1}(x - \phi(x)).$$

Hence

$$\phi(n) = |A \setminus (X \cup P)| = |A| - |X| - |P| + |X \cap P| =$$

$$= xp^a - p^a(x - \phi(x)) - xp^{a-1} + p^{a-1}(x - \phi(x))$$
$$= xp^a - xp^a + p^a\phi(x) - xp^{a-1} + xp^{a-1} - p^{a-1}\phi(x)$$
$$= p^a\phi(x) - p^{a-1}\phi(x) = \phi(x)(p^a - p^{a-1}).$$

Thus by induction on k we obtain that formula

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

hold for all n.