VE475 Homework 4

Liu Yihao 515370910207

Ex. 1 — Euler's totient

1. Suppose
$$\varphi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}$$
which means, there are p^{k-1} integers of $n \in [1, p^k]$ so that
$$\gcd(n, p^k) > 1$$
What's more, if an integer and p^k is not coprime, it can be divided by p since all of prime factors of p^k are p.

When $k = 1$, we know $\varphi(p) = p - 1$ since p is a prime.

When $k = i$, suppose $\varphi(p^i) = p^i - p^{i-1}$.

When $k = i + 1$, we know that there are p^{i-1} integers in $[1, p^i]$ which are not coprime with p^i, so they are also not coprime with p^{i+1}. Then consider the integers $n \in [p^i + 1, p^{i+1}]$ which are not coprime with p^{i+1}, we know that they all have a prime factor p, and $n/p \in [p^{i-1} + 1, p^i]$, so there are $(p-1)p^{i-1}$ integers that satisfy this condition. In total, there are $p^{i-1} + (p-1)p^{i-1} = p^i$ integers which are not coprime with p^{i+1}, so $\varphi(p^{i+1}) = p^{i+1} - p^i$.

According to the mathematical induction above, we can concluded that
$$\varphi(p^k) = p^{k-1}(p-1)$$