4 Euler's Totient Function

(a) $p - 1$

Since p is a prime number, by definition of prime numbers, so $p > 1$ and p is not divisible by any positive integer except 1 and itself, p. First, by definition of greatest common divisor, we have that $\gcd(p, 1) = 1$ and $\gcd(p, p) = p \neq 1$, which means that 1 is in the set we defined, and p is not. We proceed to prove that for any arbitrary $i \in \mathbb{N}, 1 < i < p$, we have that $\gcd(p, i) = 1$, which is equivalent to i is in the set.

Assume, for a contradiction, that $\gcd(p, i) \neq 1$. Let $\gcd(p, i) = d$, so $d > 1, d \in \mathbb{N}$ and $d \mid p$. Also, since $i < p$, so $d \neq p$, so $1 < d < p$ and $d \mid p$. But, by definition of primes, p should not be divisible by any positive integer besides 1 and p, and we reach a contradiction.

Thus, for all $i \in \mathbb{N}, 1 < i < p$, we have that $\gcd(p, i) = 1$, which means that i is in the set by definition of Euler's totient function.

Therefore, there is a total of $1 + (p - 2) = p - 1$ positive integers less than or equal to p which are relatively prime to it; in other words, $\phi(p) = p - 1$.

(b) $p^k - p^{k-1}$

Since p is a prime, so the only prime factor of p^k is p. We claim that for any integer $i\mathbb{Z}^+, 1 \leq i \leq p^k$, if i is relatively prime to p, then i is also relatively prime to p^k. We proceed by contradiction to prove the claim.

Suppose there exist an $i^*\mathbb{Z}^+, 1 \leq i^* \leq p^k$ such that i^* is relatively prime to p, but not relatively prime to p^k. Let $\gcd(p^k, i^*) = d$, so $d \in \mathbb{Z}, d > 1$. So, we have that $d \mid i^*$ and $d \mid p^k$, and since p is a prime, so d would have to divide p. Now, $d \mid p$ and $d \mid i^*$, so $\gcd(p, i^*) > d > 1$, which implies that p, i^* are not relatively prime, so we conclude with a contradiction, so our assertion above is true.

Thus, if i is in the set we defined, meaning that p^k, i are relatively prime, then p, i are also relatively prime. Using the logic from our proof in part (a), since p is a prime, so i would be relatively prime to p^k unless $p \mid i$; in other words, i is a multiple of p. For i such that $1 \leq i \leq p^k$, since $p^k = p^{k-1} * p$, so all the multiples of p are: $1 * p, 2 * p, 3 * p, ..., p^{k-1} * p$, which means that there are p^{k-1}-many multiples of p, and all other positive integers less than or equal to p^k are relatively prime to p^k. Thus, there are $p^k - p^{k-1}$ numbers relatively prime to p^k.

Therefore, there are $(p^k - p^{k-1})$-many numbers in the set defined; so in other words, $\phi(p^k) = p^k - p^{k-1}$.

(c) 1

Since p is a prime number and $a \in \mathbb{Z}^+, a < p$, using our logic in parts (a) and (b) again, so we have that a, p are relatively prime. Again, using the result from part (a), so we have that $\phi(p) = p - 1$. With the fact that we proved earlier, which is equivalent to $\gcd(p, a) = 1$, using *Fermat's Little Theorem*, so we have that $a^{\phi(p)} \equiv 1 \pmod{p}$.

(d) Direct Proof

We proceed by a direct proof. Given that $b \in \mathbb{Z}^+$ with prime factors $p_1, p_2, ..., p_k$, and $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, so we have that $p_1, p_2, ..., p_k$ are all different primes, which implies that $p_1, p_2, ..., p_k$ are all relatively prime; in other words, for any p_i, p_j with $1 \leq i, j \leq k$, so $\gcd(p_i, p_j) = 1$. Now we claim that for two different primes p_i, p_j, then for any $\alpha_i, \alpha_j \in \mathbb{N}$, we have $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$.

Assume, for a contradiction, that $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) \neq 1$, so let $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = d$ where $d \in \mathbb{Z}^+, d > 1$.

Thus, we have that $d \mid p_i^{\alpha_i}$. Since p_i is prime and $d > 1$, so d has to be a multiple of p_i. Let $d = p_i \cdot d^*, d^* \in \mathbb{Z}^+$. Since by definition of greatest common divisors, we also have that $d \mid p_j^{\alpha_j}$, so $p_i \mid p_j^{\alpha_j}$, which is impossible since p_i, p_j are different primes. Thus, we have a contradiction, so $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$.

Thus, using the given property of Euler's totient function, we have that $\phi(b) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$. Then, using the result obtained from part (b), we have that $\phi(b) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$.

Now, for any a relatively prime to b, and any arbitrary $i \in \{1, 2, ..., k\}$, we have that a, p_i is also relatively prime, which is equivalent to $\gcd(a, p_i) = 1$. Thus, *Fermat's Little Theorem*, we have that $a^{p_i - 1} \equiv 1 \pmod{p_i}$.

Therefore, $a^{\phi(b)} = a^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} = a^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_i^{(\alpha_i - 1)} \cdot (p_i - 1)) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} = a^{(p_i - 1) \cdot (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots p_i^{(\alpha_i - 1)} \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} \equiv 1^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots p_i^{(\alpha_i - 1)} \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} \equiv 1 \pmod{p_i}$.

Therefore, for any a relatively prime to b, $\forall i \in \{1, 2, ..., k\}, a^{\phi(b)} \equiv 1 \pmod{p_i}$.

Q.E.D.