PROBLEM 1.

(a) Factor 336 and use the factorization to compute $\varphi(336)$, i.e., the number of positive integers a less than 336 such that $\gcd(a, 336) = 1$.

(b) What is the remainder of $5^{960000290}$ upon division by 336?

SOLUTION:

(a) Since $336 = 2^4 \cdot 3 \cdot 7$,

$$\begin{aligned}\varphi(336) &= 336\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)\\ &= 2^4 \cdot 3 \cdot 7\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\\ &= 2^3 \cdot 1 \cdot 2 \cdot 6\\ &= 96.\end{aligned}$$

(b) By Euler's formula, we have $a^{96} \equiv 1 \pmod{336}$ if $\gcd(a, 336) = 1$. Therefore,

$$5^{960000290} \equiv 5^{960000000+290} \equiv 5^{960000000}5^{290} \equiv 5^{290} \pmod{336}.$$

Since the remainder of 290 upon division by 96 is 2, we get

$$5^{960000290} \equiv 5^{290} \equiv 5^2 \equiv 25 \pmod{336}.$$

So the remainder of $5^{960000290}$ upon division by 336 is 25.

PROBLEM 2 (Sketch of probabilistic proof of Euler's formula for the totient function.). Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of the positive integer n. Let $[n] := \{1, \ldots, n\}$ be our sample space with uniform distribution. For $i = 1, \ldots, k$, define the event E_i to be the set of $r \in [n]$ such that $p_i \nmid r$.

(a) What are the sets E_i in the case $n = 60$? What are the probabilities $P(E_i)$?

(b) Back to the case of general n, what is $P(E_i)$ for each i?

(c) Let R be the collection of $r \in [n]$ which are relatively prime to n. Check that $R = E_1 \cap E_2 \cap \cdots \cap E_k$.

(d) It turns out that $P(R) = P(E_1) \cdots P(E_k)$. Use this fact to prove that

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

SOLUTION:

(a) In this case, $p_1 = 2, p_2 = 3$ and $p_3 = 5$.

$$\begin{aligned}
E_1 &= [60] \setminus \{2, 4, 6, 8, \dots, 60\} \\
E_2 &= [60] \setminus \{3, 6, 9, 12, \dots, 60\} \\
E_3 &= [60] \setminus \{5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60\} .
\end{aligned}$$

Therefore,

$$\begin{aligned}
P(E_1) &= \frac{|E_1|}{60} = 1 - \frac{60/2}{60} = 1 - \frac{30}{60} = 1 - \frac{1}{2} \\
P(E_2) &= \frac{|E_2|}{60} = 1 - \frac{60/3}{60} = 1 - \frac{20}{60} = 1 - \frac{1}{3} \\
P(E_3) &= \frac{|E_3|}{60} = 1 - \frac{60/5}{60} = 1 - \frac{12}{60} = 1 - \frac{1}{5}.
\end{aligned}$$

(b) $P(E_i) = 1 - \frac{1}{p_i}$.

(c) A number is not relatively prime to n if and only if it is divisible by at least one of $p_1, \dots, p_k$. The result follows.

(d) The probability a number in $[n]$ is relatively prime to n is

$$\frac{|R|}{n} = P(R) = \prod_{i=1}^{k} P(E_i) = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Since $|R| = \varphi(n)$, the result follows.

PROBLEM 3. For each $k \in \{1, 2, 3, 4\}$, find all numbers n such that $\varphi(n) = k$.

SOLUTION: Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n. Then

$$\begin{aligned}
\varphi(n) &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\
&= n \prod_{i=1}^{k} \left(\frac{p_i - 1}{p_i}\right) \\
&= p_1^{e_1} \cdots p_k^{e_k} \prod_{i=1}^{k} \left(\frac{p_i - 1}{p_i}\right) \\
&= p_1^{e_1 - 1} \cdots p_k^{e_k - 1} \prod_{i=1}^{k} (p_i - 1).
\end{aligned}$$

Reasoning from this formula, it follows that $\varphi(n) = 1$ if and only if $n \in \{1,2\}$.

$$\varphi(n) = \begin{cases} 1 & \text{if and only if } n \in \{1,2\} \\ 2 & \text{if and only if } n \in \{3,4,6\} \\ 3 & \text{never} \\ 4 & \text{if and only if } n \in \{5,8,10,12\}. \end{cases}$$

PROBLEM 4. How does Euler's formula show that if $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$? Find the smallest integers a and b such that $\varphi(ab) \neq \varphi(a)\varphi(b)$.

SOLUTION: Suppose $\gcd(m,n) = 1$. Let $m = p_1^{m_1} \cdots p_k^{m_k}$ and $n = q_1^{n_1} \cdots q_\ell^{n_\ell}$ be prime factorizations. Then the prime factorization of mn is $p_1^{m_1} \cdots p_k^{m_k} q_1^{n_1} \cdots q_\ell^{n_\ell}$. The result then follows immediately from Euler's formula for the φ function.

The smallest integers a, b for which $\varphi(ab) \neq \varphi(a)\varphi(b)$ are $a = b = 2$. In that case $\varphi(2 \cdot 2) = \varphi(4) = 2 \neq \varphi(2)\varphi(2) = 1$.

PROBLEM 5. Describe the positive integers n for which $\varphi(n)|n$.

SOLUTION: Using Euler's formula for φ, we have

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

The factors on the right come from among

$$\frac{2}{1}, \frac{3}{2}, \frac{5}{4}, \frac{7}{6}, \frac{11}{10}, \frac{13}{12}, \ldots$$

Considering the 2s in the denominators, we see that we can have at most one factor of the form $\frac{p}{p-1}$ with $p > 2$, in which case the factor $\frac{2}{1}$ must also appear. So if some $p > 2$ is involved, we would have

$$\frac{2}{1}\frac{p}{p-1} \in \mathbb{Z},$$

which forces $p = 3$. Therefore, $\varphi(n)|n$ if and only if

$$n = 2^i 3^j$$

with the condition that if $j > 0$, then $i \geq 1$.