Problem 1. Let p, q be distinct prime numbers. Prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} .$$

Solution: Since $p \neq q$ are prime numbers, we have $\gcd(p, q) = 1$. By Fermat's Little Theorem, $p^{q-1} \equiv 1 \pmod{q}$. Clearly $q^{p-1} \equiv 0 \pmod{q}$. Thus

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q} .$$

Exchanging the roles of p and q in the above argument, we prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p} .$$

In other words, $p^{q-1} + q^{p-1} - 1$ is divisible by both p and q. Since p and q are relatively prime, we conclude that $p^{q-1}+q^{p-1}-1$ is divisible by pq, i.e. $p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$.

Problem 2. Let m, n be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and that $\phi(mn) = m\phi(n)$

Solution: Since $m|n$, we can number the prime divisors of n such that

$$m = p_1^{a_1}...p_s^{a_s} \text{ and } n = p_1^{b_1}...p_s^{b_s}p_{s+1}^{b_{s+1}}...p_t^{b_t},$$

where $t \geq s$, $0 < a_i \leq b_i$ for $i = 1, 2, ..., s$ and $0 < b_i$ for $i > s$, and $p_1, ..., p_t$ are pairwise distinct prime numbers.

Now

$$\phi(m) = (p_1 - 1)p_1^{a_1-1}...(p_s - 1)p_s^{a_s-1}$$

and

$$\phi(n) = (p_1 - 1)p_1^{b_1-1}...(p_s - 1)p_s^{b_s-1}(p_{s+1} - 1)p^{b_{s+1}-1}...(p_t - 1)p_t^{b_t-1}.$$

It is clear now that $\phi(m)|\phi(n)$. Moreover, $mn = p_1^{a_1+b_1}...p_s^{a_s+b_s}p_{s+1}^{b_{s+1}}...p_t^{b_t}$ and

$$\phi(mn) = (p_1 - 1)p_1^{a_1+b_1-1}...(p_s - 1)p_s^{a_s+b_s-1}(p_{s+1} - 1)p^{b_{s+1}-1}...(p_t - 1)p_t^{b_t-1} = m\phi(n).$$

Second solution: Suppose that the result is false and let $m|n$ be a counterexample with smallest possible n. Clerly $m > 1$ (since the result holds trivially for $m = 1$). Let p be a prime divisor of m. Thus we can write $m = p^a m_1$ and $n = p^b n_1$ for some

$0 < a \leq b$ and natural numbers n_1, m_1 not divisible by p. Since $m_1 | n = p^b n_1$ and $\gcd(p, m_1) = 1$, we have $m_1 | n_1$. Also

$$\phi(m) = \phi(p^a)\phi(m_1) = (p-1)p^{a-1}\phi(m_1),$$

$$\phi(n) = \phi(p^b)\phi(n_1) = (p-1)p^{b-1}\phi(n_1)$$

and

$$\phi(mn) = \phi(p^{a+b})\phi(m_1 n_1) = (p-1)p^{a+b-1}\phi(m_1 n_1).$$

Since $m_1 | n_1$ and $n_1 < n$, the result is true for m_1, n_1, i.e. $\phi(m_1)|\phi(n_1)$ and $\phi(m_1 n_1) = m_1 \phi(n_1)$. But then

$$\phi(m) = (p-1)p^{a-1}\phi(m_1) | (p-1)p^{b-1}\phi(m_1) | (p-1)p^{b-1}\phi(n_1) = \phi(n)$$

and

$$\phi(mn) = (p-1)p^{a+b-1}\phi(m_1 n_1) = p^a m_1 (p-1)p^b \phi(n_1) = m\phi(n)$$

so the result is true for m, n contrary to our assumption. The contradiction proves that no counterexample to our result exists.

Problem 3. Compute $\phi(2592)$, $\phi(111111)$, $\phi(15!)$.

Solution: We have

$$2592 = 4 \cdot 648 = 4 \cdot 4 \cdot 162 = 2^5 \cdot 81 = 2^5 \cdot 3^4$$

Thus $\phi(2592) = \phi(2^5)\phi(3^4) = 2^4 \cdot 2 \cdot 3^3 = 2^5 \cdot 3^3$.

Clearly 111111 is divisible by 11,3 so

$$111111 = 11 \cdot 10101 = 11 \cdot 3 \cdot 3367$$

Now 3367 is divisible by 7: $3367 = 7 \cdot 481$. The next prime to consider is 13 and indeed $481 = 13 \cdot 37$. Thus $111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$ and

$$\phi(111111) = \phi(3)\phi(7)\phi(11)\phi(13)\phi(37) = 2 \cdot 6 \cdot 10 \cdot 12 \cdot 36 = 2^7 \cdot 3^4 \cdot 5.$$

Finally $15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$, so

$$\phi(15!) = \phi(2^{11})\phi(3^6)\phi(5^3)\phi(7^2)\phi(11)\phi(13) = 2^{10} \cdot 2 \cdot 3^5 \cdot 4 \cdot 5^2 \cdot 6 \cdot 7 \cdot 10 \cdot 12 = 2^{17} \cdot 3^7 \cdot 5^3 \cdot 7.$$

Problem 4. Prove that 561 is a composite number and $a^{561} \equiv a \pmod{561}$ for every integer a.

Solution: Let us first note the following corollary from Fermat's Little Theorem:

Proposition 1. *Let p be a prime number. For any integer n and any natural number k we have $n^{k(p-1)+1} \equiv n \pmod{p}$.*

Indeed, if $p|a$ then both sides of the congruence are $\equiv 0 \pmod{p}$ and if $\gcd(p,a) = 1$ then $n^{p-1} \equiv 1 \pmod{p}$ and $n^{k(p-1)+1} = n(n^{p-1})^k \equiv n \pmod{p}$.

We have $561 = 3 \cdot 187 = 3 \cdot 11 \cdot 17$, so 561 is not a prime. Now $561 = 280 \cdot 2 + 1 = 56 \cdot 10 + 1 = 35 \cdot 16 + 1$. By the proposition, $n^{561} \equiv n \pmod{3}$, $n^{561} \equiv n \pmod{11}$ and $n^{561} \equiv n \pmod{17}$ for every integer n. Thus $n^{561} - n$ is divisible by 3, 11, 17 and since these numbers are pairwise relatively prime, $3 \cdot 11 \cdot 17 | n^{561} - n$, i.e. $n^{561} \equiv n \pmod{561}$ for every integer n.