1. Suppose that $n > 2$ and $c_1, \ldots, c_{\varphi(n)}$ is a reduced residue system modulo n. Show that

$$c_1 + c_2 + \cdots + c_{\varphi(n)} \equiv 0 \mod n$$

For each $1 \leqslant i \leqslant \varphi(n)$, the integer c_i is relatively prime to n. Hence, $-c_i$ is also relatively prime to n and since $c_1, \ldots, c_{\varphi(n)}$ is a reduced residue system modulo n, there must exist a j with $1 \leqslant j \leqslant \varphi(n)$ so that $c_j \equiv -c_i \mod n$. Note that we cannot have $j = i$ since if we did, we would have $2c_i \equiv 0 \mod n$ implying that $2 \equiv 0 \mod n$ since c_i is relatively prime to the modulus n. This is a contradiction since $n > 2$.

Therefore, for each $1 \leqslant i \leqslant \varphi(n)$, there exists a $j \neq i$ so that $c_i + c_j \equiv 0 \mod n$. Without loss of generality, we can assume that $c_{2k+1} + c_{2k+2} \equiv 0 \mod n$ for each $0 \leqslant k \leqslant \frac{\varphi(n)}{2} - 1$. But this immediately implies that

$$(c_1 + c_2) + (c_3 + c_4) + \cdots + (c_{\varphi(n)-1} + c_{\varphi(n)}) \equiv 0 \mod n$$

2. Suppose that a and b are relatively prime integers greater than 1. Show that $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod ab$

   Since $(a, b) = 1$, Euler's theorem implies that $a^{\varphi(b)} \equiv 1 \mod b$ and $b^{\varphi(a)} \equiv 1 \mod a$. Moreover, $a^{\varphi(b)} \equiv 0 \mod a$ and $b^{\varphi(a)} \equiv 0 \mod b$. Hence, $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod a$ and $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod b$. Since a and b are relatively prime, we can apply Sun-Tsu's theorem to acquire

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod ab$$

3. Find all positive integers n such that $\varphi(n) = 12$. Be sure to prove that you have found all solutions.

Let $n = p_1^{e_1} \cdots p_g^{e_g}$ where $p_1, \ldots, p_g$ are distinct primes and $e_1, \ldots, e_g \geqslant 1$. Suppose further that $\varphi(n) = 12$. Then we can conclude that

$$(p_1 - 1)p_1^{e_1 - 1} \cdots (p_g - 1)p_g^{e_g - 1} = \varphi(n) = 12$$

As a consequence, if for any i, $e_i > 1$, then we must have $p_i \mid 12$. This means that the only prime divisors of n which can have exponents greater than 1 are 2 and 3. Now suppose that some p_i is neither 2, nor 3. Then $p_i - 1$ must divide 12 so $p_i = 5$, $p_i = 7$, or $p_i = 13$. We now have the following cases.

<u>Case 1:</u> The largest prime factor of n is 13.

Without loss of generality, we may assume that $p_1 = 13$. We have already shown that 13 cannot have an exponent greater than 1, so we must have $e_1 = 1$. In this case, we conclude that

$$12 = \varphi(13p_2^{e_2} \cdots p_g^{e_g}) = 12\varphi(p_2^{e_2} \cdots p_g^{e_g})$$

and so $1 = \varphi(p_2^{e_2} \cdots p_g^{e_g})$. The only integers with $\varphi(k) = 1$ however are $k = 1$ and $k = 2$, so we conclude that the only possibilities in this case are $n = 13$ or $n = 26$.

<u>Case 2:</u> The largest prime factor of n is 7.

Without loss of generality, $p_1 = 7$. We have already seen that 7 cannot have an exponent larger than 1, so $e_1 = 1$ and $12 = \varphi(7 \cdot p_2^{e_2} \cdots p_g^{e_g}) = 6\varphi(p_2^{e_2} \cdots p_g^{e_g})$. As a consequence, $2 = \varphi(p_2^{e_2} \cdots p_g^{e_g})$. The only integers k with $\varphi(k) = 2$ are $k = 3$, $k = 4$, and $k = 6$, so the only possible values of n are $21, 28,$ and 42.

<u>Case 3:</u> The largest prime factor of n is 5.

Without loss of generality, $p_1 = 5$. We have already seen that 5 cannot have an exponent larger than 1, so $e_1 = 1$ and $12 = \varphi(5 \cdot p_2^{e_2} \cdots p_g^{e_g}) = 4 \cdot \varphi(p_2^{e_2} \cdots p_g^{e_g})$. As a consequence, $3 = \varphi(p_2^{e_2} \cdots p_g^{e_g})$. Since $\varphi(k)$ is always even for every integer k, there are no possible values of n in this case.

<u>Case 4:</u> The only prime factors of n are 2 and 3.

In this case, $n = 2^a \cdot 3^b$ for some $a, b \geqslant 0$, so

$$12 = \varphi(n) = 2^{a-1} \cdot 2 \cdot 3^{b-1} = 2^a \cdot 3^{b-1}$$

Hence, $a = b = 2$ so $n = 36$.

These are all of the possible cases, so the only values of n with $\varphi(n) = 12$ are $13, 21, 26, 28, 36,$ and 42.

4. For which integers $n \geqslant 2$ does $\varphi(n) \mid n$?

Suppose that $\varphi(n) \mid n$ and write $n = p_1^{e_1} \cdots p_g^{e_g}$ for distinct primes $p_1, \ldots, p_g$ and $e_1, \ldots, e_g > 0$. In particular, order the p_i so that $p_1 < p_2 < \cdots < p_g$. Moreover, under the assumption that $\varphi(n) \mid n$, we find that

$$p_1^{e_1-1} p_2^{e_2-2} \cdots p_g^{e_3-1}(p_1 - 1) \cdots (p_g - 1) \mid p_1^{e_1} \cdots p_g^{e_g}$$

and so in fact,

$$(p_1 - 1) \cdots (p_g - 1) \mid p_1 \cdots p_g$$

In particular, $p_1 - 1 \mid p_1 \cdots p_g$. If $p_1 - 1 > 1$, this is a contradiction because $p_1 - 1 < p_1 < p_2 < \cdots < p_g$. Hence, $p_1 - 1 = 1$, so $p_1 = 2$.

If 2 is the only prime factor of n, then we note that

$$\varphi(n) = \varphi(2^{e_1}) = 2^{e_1-1} \mid 2^{e_1} = n$$

as desired.

Now suppose that n has more than 1 prime factor. We have already shown that it must be the case that $p_1 = 1$. Now $p_2 - 1 \mid 2 \cdot p_2 \cdots p_g$. Since $p_2 - 1 < p_2 < p_3 < \cdots < p_g$, we must have $p_2 - 1 \mid 2$ and so $p_2 = 3$.

If 2 and 3 are the only prime factors of n, then we note that

$$\varphi(n) = 2^{e_1-1} \cdot 2 \cdot 3^{e_2-1} = 2^{e_1} \cdot 3^{e_2-1} \mid 2^{e_1} \cdot 3^{e_2} = n$$

as desired.

Now suppose for sake of contradiction that n has more than 2 prime factors. We have already shown that it must be the case that $p_1 = 2$ and $p_2 = 3$. Now, $p_3 - 1 \mid 2 \cdot 3 \cdot p_3 \cdots p_g$. Since $p_3 - 1 < p_3 < \cdots < p_g$, we must have $p_3 - 1 \mid 6$, i.e. $p_3 = 7$. However, this is impossible because

$$\varphi(2^{e_1} 3^{e_2} 7^{e_3} p_4^{e_4} \cdots p_g^{e_g}) = 2^{e_1-1} \cdot 2 \cdot 3^{e_2-1} \cdot 6 \cdot 7^{e_3-1} \cdot \varphi(p_4^{e_4} \cdots p_g^{e_g}) = 2^{e_1+1} \cdot 3^{e_2} \cdot 7^{e_3-1} \cdot \varphi(p_4^{e_4} \cdots p_g^{e_g})$$

and so $\varphi(n)$ is divisible by 2^{e_1+1}, but n is not. Hence, n cannot have more than 2 prime factors.

Therefore, the only n for which $\varphi(n) \mid n$ are the integers $n = 2^a 3^b$ where $a \geqslant 1$ and $b \geqslant 0$.

5. (Extra Credit—and don't use the internet for this one) Prove that $\lim_{n\to\infty} \varphi(n) = \infty$

Recall that for a sequence $\{a_n\}_{n\in\mathbb{N}} \subseteq \mathbb{R}$, the limit $\lim_{n\to\infty} a_n = \infty$ if for every $M > 0$, there exists $N \in \mathbb{N}$ so that for all $n > n$, we have $a_n \geqslant M$.

We first claim that for any $M \in \mathbb{Z}_{>0}$, there are only finitely many $n \geqslant 2$ with $\varphi(n) = M$. To see this, suppose that $n = p_1^{e_1} \cdots p_g^{e_g}$ for distinct primes $p_1, \ldots, p_g$ and $e_1, \ldots, e_g > 1$. Then

$$M = \varphi(n) = p_1^{e_1-1} \cdots p_g^{e_g-1}(p_1 - 1) \cdots (p_g - 1)$$

In particular, for any $1 \leqslant i \leqslant g$, $p_i - 1 \mid M$ and so $p_i \leqslant M + 1$. There are only finitely many primes less than M so any n with $\varphi(n) = M$ can have only finitely many prime factors.

Moreover, for any $1 \leqslant i \leqslant g$, $p_i^{e_i-1} \mid M$, so $p_i^{e_i-1} \leqslant M$. Taking logs on both sides and using the fact that $p_i \geqslant 2$, we find that

$$e_i - 1 \leqslant \frac{\log M}{\log p_i} \leqslant \frac{\log M}{\log 2}$$

so there are only finitely many possible values of the exponent e_i. Since there are finitely many possible prime factors of any n with $\varphi(n) = M$ and there are finitely many possible exponents on those prime factors, there can be only finitely many values of n which satisfy $\varphi(n) = M$.

Now we show that $\lim_{n\to\infty} \varphi(n) = \infty$. Fix an $M > 0$ and let $M' = \lceil M \rceil$. Then set

$$S = \{n > 0 : \varphi(n) \leqslant M'\}$$

Observe that

$$S = \bigcup_{k=1}^{M'} \{n > 0 : \varphi(n) = k\}$$

Since we now see that S is the finite union of finite sets, it follows that S is finite. In particular, S has a maximal element, say N. Now observe that by the definition of S, if $n > N$, then $\varphi(n) > M' \geqslant M$. But this is exactly what it means for $\lim_{n\to\infty} \varphi(n) = \infty$.