6. Since $gcd(a_i, n) = 1$ for any i, and $gcd(a, n) = 1$, it is obvious that $gcd(aa_i, n) = 1$ for any i.

We next prove that aa_i is not $\equiv aa_j \mod (n)$ if $i \neq j$. If not, $aa_i \equiv aa_j \mod (n)$, and $n|a(a_i - a_j)$. However, since $gcd(a, n) = 1$, this implies that $n|(a_i - a_j)$ or in other words $a_i \equiv a_j \mod (n)$, which is a contradiction.

This implies that if $a_1, a_2, \cdots a_{\phi(n)}$ is a reduced residue modulo n, so is $aa_1, aa_2, \cdots aa_{\phi(n)}$. This concludes the proof.

7. Consider the set of integers $< n$ that are coprime to n. Call these $a_1, a_2, \cdots a_{\phi(n)}$. Clearly these form a reduced residue system modulo n. Now for any a such that $gcd(a, n) = 1$, we know from exercise 6 above that $aa_1, aa_2, \cdots aa_{\phi(n)}$ is also a reduced residue system modulo n.

Now, for any i, $aa_i = qn + r_i$, where $0 < r_i < n$ and $gcd(r_i, n) = 1$. In other words, $r_i = a_j$ for some j. Thus, for each i, there is a unique j such that $aa_i \equiv a_j \mod (n)$.

Therefore,

$$\begin{aligned} aa_1aa_2\cdots aa_{\phi(n)} &\equiv a_1a_2\cdots a_{\phi(n)} \mod (n) \\ a^{\phi(n)}a_1a_2\cdots a_{\phi(n)} &\equiv a_1a_2\cdots a_{\phi(n)} \mod (n) \\ \therefore a^{\phi(n)} &\equiv 1 \mod (n) \end{aligned}$$

where the last line is due to the fact that we can cancel out the term $a_1a_2\cdots a_{\phi(n)}$ on both sides due to it being relatively coprime to n. This concludes the proof.

8. We know that $kx \equiv 1 \mod (p)$ must have exactly one unique solution since $gcd(k, p) = 1$. If the solution has the form $qp + r$, where $0 < r < p$, then $k(qp + r) \equiv 1 \mod (p)$, which leads to $kr \equiv 1 \mod (p)$. This proves that the there is some unique solution from the set $\{1, 2, \cdots (p - 1)\}$.

Further if $x = k$ is a solution for $kx \equiv 1 \mod (p)$, then $p|(k^2 - 1)$. i.e. $p|(k + 1)(k - 1)$. This is only possible if one of these terms is either 0 or p, which happens iff $k = 1$ or $k = p - 1$.

This concludes the proof.

9. In light of the solution to problem 8, $(p - 1)!$ can be thought of as products of pairs of integers k and b_k such that $kb_k \equiv 1 \mod (p)$, except the terms 1 and $(p-1)$, which don't have the appropriate pairing. Therefore, $(p-1)! \equiv 1(p-1) \mod (p)$ i.e. $(p - 1)! \equiv -1 \mod (p)$. This concludes the proof.

12. Consider $\binom{p}{k}$, where p is prime, and $k \in \{1, 2, \cdots (p - 1)\}$. $\binom{p}{k} = p!/(k!(p -$

$k)!)$ has the term p in the numerator, which none of the terms in the denominator divide (given that they are all smaller than p, and p is prime). Since $\binom{p}{k}$ is itself an integer, it must be an integer of the form pq for some integer $q >= 1$, and is thus divisible by p.

By the binomial theorem,

$$
\begin{aligned}
(a+1)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i \\
&= (a^p + 1) + \sum_{i=1}^{p-1} \binom{p}{i} a^i \\
\therefore (a+1)^p &\equiv (a^p + 1) \mod (p)
\end{aligned}
$$

This concludes the proof.

15. The numerator of $1 + (1/2) + \cdots (1/(p-1))$ is obtained by multiplying the expression by $(p-1)!$. The numerator can then be expressed as the sum $\sum_{k=1}^{p-1} (p-1)!/k$.

First consider the very first term in this sum. It is equal to $(p-1)!$ which is $\equiv -1 \mod (p)$ (due to problem 9, Wilson's theorem). Next consider the last term $(p-1)!/(p-1)$, which is $\equiv 1 \mod (p)$ (due to problem 9, Wilson' theorem, and because $(p-1) \equiv -1 \mod (p)$). Thus, the first and last terms cancel each other out and become $\equiv 0 \mod (p)$.

Now, onto the other terms. Consider the kth term. Given problem 8's solution, we can say that the kth term is $\equiv (p-1)b_k \mod (p)$, because we can pair of all other integers and reduce those multiples to be $\equiv 1 \mod (p)$. Putting it all together, we can say that the remaining terms are $\equiv (p-1)\sum_{k=2}^{p-2} k \mod (p)$. Let's see what this simplifies to.

$$
\begin{aligned}
&\equiv (p-1)\sum_{k=2}^{p-2} k && \mod (p) \\
&\equiv (p-1)(((p-1)(p-2)/2) - 1) && \mod (p) \\
&\equiv -1((-1)(-2)/2) - 1) && \mod (p) \\
&\equiv 0 && \mod (p)
\end{aligned}
$$

Therefore, the numerator is divisible by p. This concludes the proof.