Math 522 Exam 7 Solutions

1. Find $\tilde{a}$, the inverse of a modulo c, when $a = 10$ and $c = 123$.

   We will use the Euclidean algorithm to find a solution to $10x + 123y = 1$; then x will be the answer we seek. First, we have $123 = 12 \cdot 10 + 3$. Second, we have $10 = 3 \cdot 3 + 1$. Reversing, we have $1 = 10 - 3 \cdot 3 = 10 - 3 \cdot (123 - 12 \cdot 10) = -3 \cdot 123 + 37 \cdot 10$. Hence the desired $\tilde{a} = 37$.

2. Let $m \in \mathbb{Z}$ with $m > 2$. Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. Prove that $r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0 \pmod{m}$.

   Note that r_i is in the r.r.s. if and only if $\gcd(r_i, m) = 1$, if and only if $\gcd(-r_i, m) = 1$, if and only if there is some r_j in the r.r.s. with $r_j \equiv -r_i \pmod{m}$. In particular, $r_i + r_j \equiv 0 \pmod{n}$. If we can pair off the entire r.r.s. this way, we are done; however, it might be possible that $r_i = r_j$.

   We will now prove that $r_i \equiv -r_i \pmod{m}$ is impossible, for any i. Suppose otherwise. This holds if and only if $2r_i \equiv 0 \pmod{m}$, if and only if $m|2r_i$. But $\gcd(m, r_i) = 1$, so $m|2$, which is impossible.

   Hence, we may rearrange the r.r.s. so that $r_2 \equiv -r_1$, $r_4 \equiv -r_3, \ldots$. We now have $r_1+r_2+\cdots \equiv (r_1+r_2)+(r_3+r_4)+\cdots \equiv 0 + 0 + \cdots + 0 \equiv 0 \pmod{m}$.