Math 567, Assignment #2: Solutions

1. If $n = 1$, then $a \equiv b \pmod{n}$ for all a, b, period. If $n = 2$, then $0 \equiv 0^2$ and $1 \equiv 1^2$, so $a^2 \equiv b^2$ implies $a \equiv a^2 \equiv b^2 \equiv b$. But if $n > 2$, then we have $(-1)^2 \equiv 1^2$ but $-1 \not\equiv 1$.

2. $2^{50} = ((2^{10})^5) = (1024)^5 \equiv (2)^5 = 32 \equiv 4 \pmod{7}$, where we use the fact that $1024 \equiv 2 \pmod{7}$. $41^{65} \equiv (-1)^{65} \equiv -1 \equiv 6 \pmod{7}$.

3. Mod 223 we have $2^{36} = ((2^9)^2)^2 = ((512)^2)^2 \equiv ((66)^2)^2 = (4356)^2 \equiv (119)^2 = 14161 \equiv 112$, so $2^{37} \equiv 224 \equiv 1$ and $2^{37} - 1 \equiv 0$, as claimed.

4. Mod 4, we have $1^5 \equiv 1$, $2^5 \equiv 0$, $3^5 \equiv 3$, $4^5 \equiv 0$, $5^5 \equiv 1$, $6^5 \equiv 0$, $7^5 \equiv 3$, $8^5 \equiv 0$, etc., so the whole sum is $\equiv (1 + 0 + 3 + 0) \times 25 = 4 \times 25 = 100 \equiv 0 \pmod{4}$.

5. Suppose $a_1, ..., a_n$ is a complete set of residues mod n. As Burton says (p. 64), to show that $c + a_1, ..., c + a_n$ is also a complete set of residues, it's enough to show that no two of them are congruent. But $c + a_i \equiv c + a_j$ would imply $a_i = (c + a_i) - c \equiv (c + a_j) - c \equiv a_j$, which implies $i = j$. So the claim holds.

6. (a) As in problem 5, it's enough to show that $ca_i \equiv ca_j$ implies $a_i \equiv a_j$. But $ca_i \equiv ca_j \pmod{n}$ implies $n | ca_i - ca_j = c(a_i - a_j)$, and since $\gcd(c, n) = 1$, Euclid's lemma imlies $n | a_i - a_j$, whence $a_i \equiv a_j \pmod{n}$.

(b) Assume $\gcd(c, n) = d > 1$. If $ca_1, ..., ca_n$ were a complete set of residues there would exist i such that $ca_i \equiv 1 \pmod{n}$, so that $n | ca_i - 1$. But $d | n$ and $d | ca_i$ so $d | 1$: contradiction. Alternative proof: If we take $i \neq j$ such that $a_i \equiv 0 \pmod{n}$ and $a_j \equiv \frac{n}{d} \not\equiv 0 \pmod{n}$, we get $ca_i \equiv 0 \pmod{n}$ and $ca_j \equiv \frac{cn}{d} = \frac{c}{d} n \equiv 0 \pmod{n}$, so $ca_i \equiv ca_j$. Hence $ca_1, ..., ca_n$ cannot be a complete system of residues.

7. By re-ordering if necessary, we can assume $a_1 \equiv 0$, $a_2 \equiv 1$, $a_3 \equiv 2$, $a_4 \equiv 3$, and $a_5 \equiv 4 \pmod{5}$. Then $a_1^3 \equiv 0^3 \equiv 0$, $a_2^3 \equiv 1^3 \equiv 1$, $a_3^3 \equiv 2^3 \equiv 8 \equiv 3$, $a_4^3 \equiv 3^3 \equiv 27 \equiv 2$, and $a_5^3 \equiv 4^3 \equiv 64 \equiv 4 \pmod{5}$. Since a_1^3, a_2^3, a_3^3, a_4^3, and a_5^3 are mutually non-congruent mod 5, they constitute a complete set of residues mod 5.

8. 9^{10} ends in 01, so $9^n \equiv 9^{n+10} \pmod{100}$ for all n, and in general $9^a \equiv 9^b \pmod{100}$ as long as $a \equiv b \pmod{10}$. Putting $a = 9^9 \equiv (-1)^9 = -1 \equiv 9 \pmod{10}$, we have $9^{(9^9)} \equiv 9^9 \pmod{100}$, and it is not hard to check that the last two digits of 9^9 are 89.