Math 522 Exam 6 Solutions

1. Find all solutions to $28823x \equiv 34891 (\text{mod } 56129)$.

   We first find $d = \gcd(28823, 56129)$ with the Euclidean algorithm. $56129 = 1 \cdot 28823 + 27306$, $28823 = 1 \cdot 27306 + 1517$, $27306 = 18 \cdot 1517 + 0$, so $d = 1517$. $34891/d = 23$, so this system will have d solutions. To find them, we must solve $\frac{28823}{1517}x \equiv \frac{34891}{1517} (\text{mod } \frac{56129}{1517})$, i.e. $19x \equiv 23 (\text{mod } 37)$. We must therefore find the reciprocal of 19, modulo 37. Fortunately, we don't have to look far, since $19 \cdot 2 = 38 \equiv 1 (\text{mod } 37)$. Hence $x \equiv 23 \cdot 2 = 46 \equiv 9 (\text{mod } 37)$. Hence, there are 1517 mutually incongruent solutions, equivalent to $9 + 37k$, for $k \in [0, 1517)$.

2. For all integers a_1, a_2, n_1, n_2, with $n_1, n_2 > 0$ and $\gcd(n_1, n_2) = 1$, prove that there is some integer x with $x \equiv a_1 (\text{mod } n_1)$ AND simultaneously $x \equiv a_2 (\text{mod } n_2)$.
   BONUS: extend your proof from 2 modular equations to k modular equations. (all n's are pairwise relatively prime)

   SOLUTION 1: Consider $S = \{a_1 + 1n_1, a_1 + 2n_1, a_1 + 3n_1, \ldots, a_1 + n_2 n_1\}$. If two of these (say, the i^{th} and j^{th}) are congruent mod n_2, then $n_2 | (a_1 + in_1) - (a_1 + jn_1) = (i - j)n_1$. But $\gcd(n_1, n_2) = 1$, so by Thm 2-3, $n_2 | i - j$. Since $i, j \in [1, n_2]$ we must have $i - j = 0$. This proves that S is a complete residue system modulo n_2, so in particular one element is congruent to a_2 modulo n_2. But this integer is also congruent to a_1 modulo n_1, because everything in S has this property by the construction of S.

   SOLUTION 2 (Maria, Seo Bin): Because $\gcd(n_1, n_2) = 1$, we apply Thm 2-4 (or Cor 2-2) to find b, c satisfying $bn_1 - cn_2 = a_2 - a_1$. We rearrange to get $bn_1 + a_1 = cn_2 + a_2$, and set x to be this value; it satisfies the desired congruences.

   SOLUTION 3 (just for fun): Set $x = a_1 n_2^{\phi(n_1)} + a_2 n_1^{\phi(n_2)}$ and use Euler's theorem to see that x satisfies the desired congruences.

   BONUS: We need to convert the above argument into an inductive proof. The base case is $k = 1$, which is solved with $x = a_1$. By our inductive hypothesis, we have some x that satisfies $x \equiv a_1 (\text{mod } n_1), x \equiv a_2 (\text{mod } n_2), \ldots x \equiv a_{k-1} (\text{mod } n_{k-1})$. Set $m = n_1 n_2 \cdots n_{k-1}$, and note that $m \equiv 0 (\text{mod } n_i)$ for $i \in [1, k-1]$. Hence, not only x, but $x + m, x + 2m, x + 3m, \ldots$ all satisfy the first $k - 1$ modular equations. Set $S = \{x + 1m, x + 2m, \ldots, x + n_k m\}$. If two of these are congruent mod n_k, then $n_k | (x + im) - (x + jm) = (i - j)m$. But $\gcd(x, m) = 1$, so by Thm 2-3, $n_k | (i - j)$ and hence $i - j = 0$. So S is a complete residue system modulo n_k, and hence one element is congruent to a_k modulo n_k. This completes the inductive step and the proof.

3. High score=100, Median score=75, Low score=50