Math 522 Exam 8 Solutions

1. Calculate $\phi(9,800,000)$.
   BONUS: Find all $n \in \mathbf{N}$ such that $\phi(n) = 20$.

   We factor $9,800,000 = 2^6 5^5 7^2$. *Hence* $\phi(9,800,000) = \phi(2^6)\phi(5^5)\phi(7^2) = (2^6-2^5)(5^5-5^4)(7^2-7^1) = (32)(2500)(42) = 3,360,000$.

   BONUS: We first factor twenty into natural numbers in every possible way: $20, 20\cdot 1, 10\cdot 2, 10\cdot 2\cdot 1, 5\cdot 4, 5\cdot 4\cdot 1, 5\cdot 2\cdot 2, 5\cdot 2\cdot 2\cdot 1$. *We will repeatedly use that* $\phi(p^k) = p^{k-1}(p-1)$. *We first show that* $\phi(p^k) = 1$ *only for* $p = 2, k = 1$ *[proof:* $(p-1)|1$, *so* $p - 1 = 1$*]. We next show that* $\phi(p^k) = 2$ *for* $(p = 2, k = 2)$ *and* $(p = 3, k = 1)$, *only [proof: since* $p - 1|2$, *either* $p - 1 = 1$, *or* $p - 1 = 2$*]. We next show that* $\phi(p^k)$ *never equals 5 [proof:* $p - 1 = 1$ *or* $p - 1 = 5$*]. We next show that* $\phi(p^k) = 10$ *only for* $p = 11, k = 1$ *[proof: several cases;* $p - 1 = 1, 2, 5, 10$*]. Finally, we show that* $\phi(p^k) = 20$ *only for* $p = 5, k = 2$ *[proof:* $p - 1 = 1, 2, 4, 5, 10, 20$*]. Putting this all together, we have* $\phi(25) = 20, \phi(50) = 20 \cdot 1, \phi(33) = 10 \cdot 2, \phi(44) = 10 \cdot 2, \phi(66) = 10 \cdot 2 \cdot 1$, *and no others are possible since we can't make 5.*

2. Let n be a positive integer with $n > 2$. Let R be any reduced residue system modulo n. Prove that n divides the sum of all the elements of R.

   This is essentially exercise #4 in 5-2. Please remember to keep up with your homework.

   The key is to pair off elements of R *in such a way that* n *divides the sum of each pair. We pair* $r \in R$ *with an element of* R *congruent to* $n - r$. *Note that* $f : r \to n - r$ *satisfies* $f(f(r)) = r$, *so it induces a pairing. This element is in* R, *provided that* $\gcd(n-r, n) = 1$. *There are several ways to prove this fact. One way is* $\gcd(n-r, n) = \gcd(n - r, n - (n - r)) = \gcd(n - r, r) = \gcd(n - r + r, r) = \gcd(n, r)$, *where twice we applied the theorem that* $\gcd(a, b) = \gcd(a + bk, b)$ *for any integer* k. *Another way is to note that* $\gcd(-r, n) = \gcd(r, n)$, *and that* $-r$ *is congruent to* $n - r$ *modulo* n.

   The only time this pairing will fail is if the two elements of our pairing are not different elements of R *(that is,* r *is paired with itself). One way to prove this is with exercise 4 in Sectin 6.1. Another way is directly:* $r \equiv n-r$ *implies that* n *divides* $r-(n-r) = 2r-n$. *This is equivalent to* $n|2r$. *This, in turn, is equivalent to* $r = k(n/2)$, *for some integer* k. *If* n *is odd, then* k *must be even and* $\gcd(r, n) = n$*; if* n *is even, then* $\gcd(r, n) \geq n/2$. *In any case, this is violative of* $r \in R$. *Hence* $r, n - r$ *will always be different elements of* R, *provided* $n > 2$.

3. Exam grades: 102, 97, 87, 86, 86, 85, 81, 80, 79, 76, 76, 72, 65