Math 55—Fall 2012
Homework 6 Solutions

4.3 #6. We need to figure out the largest power of 10 that divides 100!. To do this, we find the largest powers of 2 and 5 that do so. Of the numbers 1 through 100, twenty are multiples of 5. Of these, four are multiples of $25 = 5^2$. In the product, 100!, the four multiples of 25 contribute a factor 5^8, and the the other 16 multiples of 5 contriubte 5^{16}. So the largest power of 5 that divides 100! is 5^{24}. In a similar way, we can find the largest power of 2 that divides 100!, but we don't need to do this precisely: it is at least 2^{50}, since fifty of the factors are even, and this exponent is already larger than the exponent in the power of 5. Therefore, using unique factoriztion into primes, the largest power of 10 that divides 100! is $10^{24} = 2^{24}5^{24}$. In other words, 100! written in decimal ends with 24 zeroes.

4.3 #12. Following the hint, let's consider the n integers $(n+1)! + k$, as k goes from 2 to $n+1$. Since every such k divides $(n+1)!$, k divides $(n+1)! + k$, hence $(n+1)! + k$ is composite for all $2 \leq k \leq n+1$. [Note that it would also work if we used the lcm of the numbers 2 through $n+1$ in place of $(n+1)!$ in this construction.]

4.3 #28. This is easiest to do using prime factorization: $1000 = 2^3 5^3$, $625 = 5^4$, so $\gcd(1000, 625) = 5^3 = 125$, and $\text{lcm}(1000, 625) = 2^3 5^4 = 5000$. Check: $1000 \cdot 625 = 125 \cdot 5000 = 625000$.

4.3 #40(f). Leaving the details to you, the answer is $\gcd(124, 323) = 1 = -112 \cdot 124 + 43 \cdot 323$.

4.3 #50. Let $d = \gcd(a, m)$ and $e = \gcd(b, m)$. By hypothesis, m divides $a - b$, hence d divides $a - b$, and since d divides a, it follows that d divides b. Since d also divides m, d divides $e = \gcd(b, m)$. By the same reasoning with a and b swapped, e divides d. Since d and e divide each other, $d = e$.

4.3 #54. Following the hint, if $q_1, \ldots, q_n$ are primes, each $q_i \equiv -1 \pmod 3$ (which is the same as saying q_i is of the form $3k + 2$), we'll show that there is another prime $p \equiv -1 \pmod 3$ which is not one of the q_i. Then it follows that the set of all primes congruent to $-1 \pmod 3$ is infinite.

To do this, let $M = 3q_1 \cdots q_n - 1$. Since $M \equiv -1 \pmod 3$, the prime 3 is not a factor of M, and at least one prime factor p of M must have $p \equiv -1 \pmod 3$. Otherwise, all prime factors of M would be congruent to $1 \pmod 3$, which would imply $M \equiv 1 \pmod 3$. But $M \equiv -1 \pmod{q_i}$ for each q_i, so no q_i is a prime factor of M. Thus p is not one of the q_i, and the argument is complete.

4.4 #8. Let $d = \gcd(a, m) > 1$. Let $a = rd$ and $m = sd$. Note that $1 < s < m$, so $s \not\equiv 0 \pmod m$. Now $sa = rsd = rm \equiv 0 \pmod m$. If a had a multiplicative inverse modulo m, we could multiply both sides of $sa \equiv 0 \pmod m$ by a^{-1} to get $s \equiv 0 \pmod m$, a contradiction.

4.4 #12(b). Using the Euclidean algorithm, we find $1 = 89 \cdot 144 - 55 \cdot 233$, so 89 is an inverse of $144 \pmod{233}$. Multiplying by 89 on both sides of $144x \equiv 4 \pmod{233}$, we get $x \equiv 4 \cdot 89 \equiv 123 \pmod{233}$.

4.4 #24. See solution to 4.4 #21 in back of book for answer.

4.4 #32. A multiple of 5 which is congruent to 1 (mod 3) is 10. By Chinese Remainder Theorem, all the multiples of 5 which are congruent to 1 (mod 3) are the integers $x \equiv 10 \pmod{15}$.

Additional Problem. Theorem: if $n \equiv 7 \pmod{8}$, then n is not a sum of three perfect squares.

Proof. First calculate the squares of all elements of $\mathbb{Z}_8$, to conclude that every perfect square is congruent to 0, 1 or 4 (mod 8). Now observe that no sum of three of these numbers is congruent to 7 (mod 8).