Math 55: Discrete Mathematics, Fall 2008
Homework 3 Solutions

3.5: 6. There are 24 zeroes at the end of 100!. To see this, let e be the exponent of 2 and f exponent of 5 in the prime factorization of 100!. Then the largest power of 10 that divides 100! is $10^{\min(e,f)}$. To calculate f, observe that 20 of the factors in $100! = 1 \cdot 2 \cdots 100$ are multiples of 5, and of those, four (25, 50, 75, and 100) contain an extra factor of 5. Since none of them contains a factor 5^3, we get $f = 24$. Since there are 50 even factors, we see that $e \geq 50$, and therefore the minimum of e and f is 24, without further calculating e.

*18. We can assume $n > 1$, so n is not relatively prime to itself. Therefore $\phi(n)$ is equal to the number of members of the set $\{1, 2, \ldots, n-1\}$ that are relatively prime to n, and thus $\phi(n) = n - 1$ if and only if every positive integer less than n is relatively prime to n. If n is prime, then clearly this condition holds. Conversely, if the condition holds, then n has no divisor $1 < d < n$, since then d would not be relatively prime to n. So n is prime.

26. The lcm is $2^4 3^4 5 \cdot 7^{11}$ by 3.5 Theorem 5.

(B) The two possibilities for the two numbers (without regard to order) are $\{a, b\} = \{2^3 3^4 5, 2^4 3^4 5 \cdot 7^{11}\}$ or $\{a, b\} = \{2^3 3^4 5 \cdot 7^{11}, 2^4 3^4 5\}$. To see this, suppose $a = 2^{d_1} 3^{d_2} 5^{d_3} 7^{d_4}$ and $b = 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4}$. We know the minimum and the sum of each pair d_i, e_i, and that determines the pair apart from order. Specifically, $\{d_1, e_1\} = \{3, 4\}$, $d_2 = e_2 = 4$, $d_3 = e_3 = 1$, and $\{d_4, e_4\} = \{0, 11\}$. Without loss of generality, by switching a and b we can assume $d_1 = 3$. The only remaining choice is $d_4 = 0$ or 11, giving the answer above.

34. $n = 6$ is a counterexample: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$.

3.6: 22. $123^{1001} \equiv 22 \pmod{101}$. (An easier way to get this than by the algorithm is using Fermat's Little Theorem, since 101 is prime).

24(f) $\gcd(11111, 111111) = 1$. This is found after just one step of the Euclidean algorithm (if I had noticed this, I would have assigned a different problem).

30. A stronger result is that if $n = d_k \cdots d_2 d_1 d_0$ in decimal, then $n \equiv (d_0 + d_2 + \cdots) - (d_1 + d_3 + \cdots) = \sum_i (-1)^i d_i \pmod{11}$. The proof is immediate from the meaning of the decimal representation, namely $n = \sum_i 10^i d_i$, and the fact that $10 \equiv -1 \pmod{11}$.

*3.7: 8. $144^{-1} \equiv 89 \pmod{233}$

10. Suppose a has inverse s modulo m, that is, $1 \equiv sa \pmod{m}$. Then $m | 1 - sa$, so there is an integer t such that $1 = sa + tm$. If $gcd(a, m) = d$, then d divides $sa + tm$, so $d = 1$.

20. The solution is $x \equiv 23 \pmod{30}$. The given congruences do not have pairwise relatively prime moduli, but we can construct from them another system of congruences that do, as follows: the first two of the given congruences imply $x \equiv 1 \pmod{2}$, the second two imply $x \equiv 3 \pmod{5}$, and the first and third imply $x \equiv 2 \pmod{3}$. Now we can apply the Chinese Remainder Theorem and find that the solution of of these three new congruences is $x \equiv 23 \pmod{30}$. Therefore any solution of the three given congruences also satisfies $x \equiv 23 \pmod{30}$, and one checks immediately that, conversely, any such x is a solution of the three given conguences.

*[5 pts each part] 28(a) $3^{302} \equiv 3^2 \equiv 4 \pmod 5$, $3^{302} \equiv 3^2 \equiv 2 \pmod 7$, $3^{302} \equiv 3^2 \equiv 9 \pmod{11}$.

(b) Since $9 \equiv 4 \pmod 5$, $9 \equiv 2 \pmod 7$, $9 \equiv 9 \pmod{11}$, the Chinese Remainder Theorem implies that $3^{302} \equiv 9 \pmod{5 \cdot 7 \cdot 11}$.

52. The quadratic residues modulo 11 are $\{1, 3, 4, 5, 9\}$.

54. We use the result from Exercise 53: for each $a \not\equiv 0 \pmod p$, if there is an x such that $x^2 \equiv a \pmod p$, that is, if a is a quadratic residue, then there are exactly two solutions modulo p of the congruence $x^2 \equiv a \pmod p$, namely x and $-x$. Another way to say the same thing is that the function $f(x) = x^2 \underline{\bmod}\, p$ maps the set $S = \{1, 2, \ldots, p-1\}$ surjectively onto the set of quadratic residues, and maps exactly 2 elements of S onto each quadratic residue. Hence the number of quadratic residues is one-half the number of elements of S, or $(p-1)/2$.

*Chapter 3 Supplementary Exercise 40 (p. 260). Suppose (x, y) were an integer solution to $x^2 - 5y^2 = 2$. Then $x^2 \equiv 2 \pmod 5$. But the quadratic residues modulo 5 are $\{1, 4\}$, so this has no solution.