Math 567, Assignment #7: Solutions

1. Using the notation introduced in class, we have $D(4) = P(1)+P(2)+P(4)$, where $P(n)$ denotes the number of primitive necklaces with n beads (each of which can be any of 3 colors). We showed that $P(n) = \frac{1}{n}\sum_{d|n} a^d \mu(n/d)$, where a is the number of colors; here $a = 3$, so $P(1) = \frac{1}{1}(3^1) = 3$, $P(2) = \frac{1}{2}(3^2 - 3^1) = 3$, and $P(4) = \frac{1}{4}(3^4 - 3^2) = 18$, so $D(4) = 3 + 3 + 18 = 24$.

2. The base 2 is relatively prime to the modulus 77, and $\phi(77) = (7-1)(11-1) = 60$, so $2^a \equiv 2^b \pmod{77}$ whenever $a \equiv b \pmod{60}$. Since $100000 \equiv 40 \pmod{60}$, we know that $2^{100000} \equiv 2^{40} \pmod{77}$. Starting from $2^5 \equiv 32 \pmod{77}$ and using repeated squaring mod 77, we get $2^{10} \equiv 32^2 \equiv 23 \pmod{77}$, $2^{20} \equiv 23^2 \equiv 67 \pmod{77}$, and $2^{40} \equiv 67^2 \equiv 23 \pmod{77}$.

3. Since the base 9 is relatively prime to the modulus 100, $9^{9^{9^9}}$ is congruent to 9^a modulo 100, where a is any number congruent to the exponent 9^{9^9} modulo $\phi(100) = (4-2)(25-5) = 40$. For simplicity of calculation, we may as well take a to be the remainder when 9^{9^9} is divided by 40. Now we must find a. In this sub-problem, the base 9 is relatively prime to the modulus 40, so 9^{9^9} is congruent to 9^b modulo 40, where b is any number congruent to the exponent 9^9 modulo $\phi(40) = (8-4)(5-1) = 16$. At this point we could just compute 9^9 modulo 16 directly, but we can also turn the crank one more time to find b: The base 9 is relatively prime to the modulus 16, so 9^9 is congruent to 9^c modulo 16, where c is any number congruent to the exponent 9 modulo $\phi(16) = 16 - 8 = 8$.

Now we can unwind what we have done: $c = 1$; $9^9 \equiv 9^c \equiv 9^1 \equiv 9$ (modulo 16); $b = 9$; $9^{9^9} \equiv 9^b \equiv 9^9$ (modulo 40). To work out 9^9 mod 40, I'll use the Chinese remainder theorem: mod 8, $9^9 \equiv 1^9 \equiv 1$, and mod 5, $9^2 \equiv 4^2 \equiv 16 \equiv 1$ and $9^9 \equiv 4^9 \equiv (4^2)^4 \cdot 4 \equiv 4$. Since $9^9 \equiv 1 \pmod 8$ and $9^9 \equiv 4 \pmod 5$, we have $9^9 \equiv 9 \pmod{40}$. Thus $a = 9$. Lastly, to work out $9^a = 9^9$ mod 100, we could resort to a calculator, or we could recall that we already worked this out on an earlier problem set, or we could use the Chinese remainder theorem. I'll take the third of these approaches: mod 4, $9^9 \equiv 1^9 \equiv 1$, and mod 25, we progressively calcualte $9^2 \equiv 81 \equiv 6$, $9^3 \equiv (9^2) \cdot 9 \equiv 6 \cdot 9 \equiv 54 \equiv 4$, and $9^9 \equiv (9^3)^3 \equiv 4^3 \equiv 64 \equiv 14$. Since $9^9 \equiv 1 \pmod 4$ and $9^9 \equiv 14 \pmod{25}$, we get $9^9 \equiv 89 \pmod{100}$. Hence the last two digits of the original number are 89.

4. If $n = 2^k$, $\phi(n) = 2^k - 2^{k-1} = n/2$, and if $n = 2^j \cdot 3^k$, $\phi(n) = (2^j -$

$2^{j-1})(3^k - 3^{k-1}) = (1/2)2^j(2/3)3^k = n/3$. However, recall the general formula $\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$. The only way to achieve $\phi(n) = n/4$ is to find a finite collection of primes p_i such that the product $P = \prod_i(\frac{p_i-1}{p_i})$ is equal to $1/4$. But this cannot happen. Indeed, given any finite collection of primes p_i, of which the largest is p_r (say), we see that none of the numerators $p_i - 1$ has a factor of p_r, whence there must be a factor of p_r in the denominator of P. But if $P = 1/4$, we must have $p_r = 2$. That is: the largest prime dividing n is 2, so that n is a power of 2. But in this case we get $\prod_i \frac{p_i-1}{p_i} = 1/2$, not $1/4$.

Alex Miller (in office hours) suggested another proof: $1/4 = \prod_i(\frac{p_i-1}{p_i})$ would imply, by cross-multiplying, $\prod_i p_i = 4\prod_i(p_i-1) = 2^2\prod_i(p_i-1)$. This contradicts the fundamental theorem of arithmetic (aka unique factorization into primes), since the left hand side is a product of distinct primes whereas the right hand side is not (the prime 2 occurs at least twice).

5. We are told that $853x \equiv 135813 \pmod{1000000}$. To solve for x, we need to find a multiplicative inverse of 853 modulo 1000000. Using the hint that 853 divides 3000001, we see that $3000001/853 = 3517$ is a multiplicative inverse of 853 modulo 1000000. So, multiplying both sides of the original congruence by 3517, we get $x \equiv 135813 \times 3517 \equiv 654321 \pmod{1000000}$.

6. We are told that $x^{89} \equiv 247 \pmod{1000}$. We want to find a number k such that $(x^{89})^k \equiv x^{89k} \equiv x \pmod{1000}$ whenever x is relatively prime to 1000, since this will enable us to determine x by calculating 247^k. Euler's theorem tells us that $x^{400} \equiv x^{\phi(1000)} \equiv 1 \pmod{1000}$ for all x relatively prime to 1000, which implies that $x^{400j+1} \equiv x \pmod{1000}$. So we are trying to find j, k with $400j + 1 = 89k$. As it happens, $(j,k) = (2,9)$ works. So $x \equiv 247^9 \equiv (247^3)^3 \equiv 223^3 \equiv 567 \pmod{1000}$.

7. (a) Use the repeated squarings trick: $560^1 \equiv 560 \pmod{3233}$, $567^2 \equiv 3232 \equiv -1 \pmod{3233}$, $567^4 \equiv 1 \pmod{3233}$, $567^8 \equiv 1 \pmod{3233}$, etc. We aren't usually so lucky! In this case, we can avoid a lot of calculation: $560^{1063} \equiv (560^4)^{265}(560^2)(560^1) \equiv (1)^{265}(-1)(560) \equiv 2673 \pmod{3233}$. The encrypted message is 2673.

(b) Since 3233 factors as 53 times 61, $\phi(3233) = (52)(60) = 3120$. So we need to find a multiplicative inverse for 1063 modulo 3120. Using the Euclidean algorithm to solve $1063x \equiv 1 \pmod{3720}$ (as described in the section on solving linear congruences), we find that $x = 1447$ works. (Details:

the successive numbers we get from the Euclidean algorithm are 3120, 1063, $3120 - 2 \cdot 1063 = 994$, $1063 - 994 = 69$, $994 - 14 \cdot 69 = 28$, $69 - 2 \cdot 28 = 13$, $28 - 2 \cdot 13 = 2$, and $13 - 6 \cdot 2 = 1$. Unwrapping, we get $1 = 13 - 6 \cdot 2 = 13 - 6 \cdot (28 - 2 \cdot 13) = -6 \cdot 28 + 13 \cdot 13 = -6 \cdot 28 + 13 \cdot (69 - 2 \cdot 28) = 13 \cdot 69 - 32 \cdot 28 = 13 \cdot 69 - 32 \cdot (994 - 14 \cdot 69) = -32 \cdot 994 + 461 \cdot 69 = -32 \cdot 994 + 461 \cdot (1063 - 994) = 461 \cdot 1063 - 493 \cdot 994 = 461 \cdot 1063 - 493 \cdot (3120 - 2 \cdot 1063) = -493 \cdot 3120 + 1447 \cdot 1063$.)

(c) To raise 2673 to the 1447 power (mod 3233), recall that $2673 \equiv -560 \pmod{3233}$; hence $2673^2 \equiv (-560)^2 \equiv 560^2 \equiv -1 \pmod{3233}$ and $2673^4 \equiv (-1)^2 \equiv 1 \pmod{3233}$. So 2673 raised to the 1444th power (mod 3233) is 1 (because 1444 is a multiple of 4), and 2673 raised to the 1447th power (mod 3233) is 2673 cubed, or $2673^2 \cdot 2673 \equiv (-1)(-560) \equiv 560 \pmod{3233}$. So we get 560 back again, as we ought. (Note, by the way, that our code would be a rather bad one if the encrypted version of x were frequently $-x$ (mod 3233), or worse, x itself! Fortunately, this doesn't usually happen; I only chose a situation like this to make the arithmetic easier for you.)

8. As discussed in class, we have $p + q = n - \phi(n) + 1 = 1914$ and $p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{1914^2 - 4 \cdot 243449} = 1640$, where p and q represent the larger and smaller primes, respectively. Thus $p = (1914 + 1640)/2 = 1777$ and $q = (1914 - 1640)/2 = 137$.