CS111 Practice Quiz 2 Solutions (version 2)

Problem 1: Compute the values described below, following the instructions. You need to show all your work (write the solutions step-by-step) in order to receive credit.

(a) The lists of multiples of 5 and 16 are:

	1	2	3	4	5	6	7	8	9	10	11	12	13
multiples of 5:	5	10	15	20	25	30	35	40	45	50	55	60	65
multiples of 16:	16	32	48	64									

So $5^{-1} \pmod{16} = 13$.

(b) Using Fermat's theorem, $3^{-1} \equiv 3^{21} \pmod{23}$. Thus, computing module 23 we have

$$3^{21} \equiv 3 \cdot 9^{10} \equiv 3 \cdot (81)^5 \equiv 3 \cdot 12^5 \equiv 3 \cdot 12 \cdot (144)^2 \equiv 36 \cdot 6^2 \equiv 13 \cdot 36 \equiv 13 \cdot 13 \equiv 169 \equiv 8.$$

(c) Computing modulo 17, we have $5^{160322} \equiv 5^{160320} \cdot 5^2 \equiv (5^{16})^{10020} \cdot 25 \equiv 1 \cdot 25 \equiv 8$.

(d) Rearranging, we get $5x \equiv -7 \pmod{16}$, which is the same as $5x \equiv 9 \pmod{16}$. Since $5^{-1} \pmod{16} = 13$ (from (a)), computing modulo 16 we get $x \equiv 9 \cdot 13 \equiv 117 \equiv 5$.

Problem 2: (a) Yes, they are different primes.

(b) $n = pq = 161$, $\phi(n) = 132$.

(c) Values $10, 11, 12, 14, 15$ are not valid, because they are not relatively prime to 132. Value 13 is correct, because it is relatively prime to 132.

(d) These values are correct, because $e = 5$ is relatively prime to 132 and $e \cdot d \equiv 265 \equiv 1 \pmod{132}$.

(e) Computing modulo 161, we get $M^e \equiv 4^5 \equiv 4 \cdot 16^2 \equiv 4 \cdot 256 \equiv 4 \cdot 95 \equiv 380 \equiv 58$.