115 Homework 8

Due MONDAY November 29

Question 1 Draw a table showing why $\phi(7)\phi(3) = \phi(21)$. Indicate what features apply to any pairs of relatively prime integers m and n.

Solution Looking at the following table:

$$\begin{array}{ccccccc} 1 & 4 & 7 & 10 & 13 & 16 & 19 \\ 2 & 5 & 8 & 11 & 14 & 17 & 20 \\ 3 & 6 & 9 & 12 & 15 & 18 & 21 \end{array}$$

We can strike out the third row since all those numbers have a factor of 3 and are therefore not relatively prime to 21. So we are left with 6 numbers in each of the first 2 rows (7 in the first row and 14 in the second row are not relatively prime to 21) so that $\phi(21) = 12 = 2 \cdot 6 = \phi(3)\phi(7)$. FOr relatively prime integers $n < m$ we can always write all integers between 1 and $m \cdot n$ as in the table above, in n rows of length m. crossinf out the elements relatively prime to $m \cdot n$ we are left with exactly $\phi(n)$ rows, each containing exactly $\phi(m)$ relatively prime elements.

Question 2 (Rosen 6.3.6) Find the last digit (base 10) of $3^{999,999}$.

Solution Since $\phi(10) = 4$, we have by Euler's theorem, $3^{999999} \equiv (3^{4 \cdot 249999+3} \equiv (3^4)^{249999} \cdot 3^3 \equiv 1 \cdot 27 \equiv 7$ (mod 10). Therefore the last decimal digit of 3^{999999} is 7.

Or if you did the problem in the book: Since $\phi(10) = 4$, we have by Euler's theorem, $7^{999999} \equiv (7^{4 \cdot 249999+3} \equiv (7^4)^{249999} \cdot 7^3 \equiv 1 \cdot 343 \equiv 3$ (mod 10). Therefore the last decimal digit of 7^{999999} is 3.

Question 3 (Rosen 6.3.10) Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \bmod ab$ if $(a, b) = 1$ and $a, b \in \mathbb{N}$.

Solution Suppose that a and b are relatively prime positive integers. Then by Euler's theorem $a^{\phi(b)} \equiv 1$ (mod b) and $b^{\phi(a)} \equiv 1$ (mod a). Since $a^{\phi(b)} \equiv 0$ (mod a) and $b^{\phi(a)} \equiv 0$ (mod b) it follows that $a^{\phi(b)} + b^{\phi(a)} \equiv 1$ (mod a), and $a^{\phi(b)} + b^{\phi(a)} \equiv 1$ (mod b). Now by the Chineses remainder theorem, since a and b are relatively prime it follows that $a^{\phi(b)} + b^{\phi(a)} \equiv 1$ (mod ab).

Question 4 (Rosen 7.1.8) Show $\nexists\, n \in \mathbb{N}$ such that $\phi(n) = 14$.

Solution If $\phi(n) = 14$, then 7, a prime factor of 14 is such that $7|p_1^{a_1} - p_1^{a_1-1}$ for some odd prime p_1. Since the only factors of 14 are 2 and 7, either $p_1 = 7$ and $a_1 > 1$ and hence $p_1 - 1 = 6|14$ is false, or $7|p_1 - 1$, but $p_1 - 1$ is even, so $p_1 - 1 = 14$ or $p_1 = 15$ which is not prime. Therefore there are no solutions.

Question 5 (Rosen 7.1.18) If $m, k \in \mathbb{N}$, show $\phi(m^k) = m^{k-1}\phi(m)$.

Solution Suppose that the prime factorization of m is $m = \prod_{i=1}^r p_i^{a_i}$. Then $\phi(m) = \prod_{i=1}^r \phi(p_i^{a_i})$. Since $m^k = \prod_{i=1}^r p_i^{ka_i}$, $\phi(m^k) = \prod_{i=1}^r \phi(p_i^{ka_i})$. Note that $\phi(p_i^{ka_i}) = p_i^{ka_i-1}(p_i-1) = p_i^{(k-1)a_i} p_i^{a_i-1}(p_i-1) = p_i^{(k-1)a_i}\phi(p_i^{a_i})$. Hence $\phi(m^k) = \prod_{i=1}^r p_i^{(k-1)a_i}\phi(p_i^{a_i}) = \prod_{i=1}^r p_i^{(k-1)a_i} \prod_{i=1}^r \phi(p_i^{a_i}) = m^{k-1}\phi(m)$.