115 Homework 10

Not for grading, solutions posted next week

Question 1 Prove there are infinitely many solutions to $\tau(n) = 2$.

Solution We have that $\tau(p) = 2$ where p is a prime number. There are an infinite number of primes thus there are infinitely many solutions to $\tau(n) = 2$.

Question 2 Consider the RSA encryption system with $n = 65$. Find the decryption key d for $e = 5$ and for $e = 7$. Encrypt the message $P = 03$ with $e = 5$.

Solution (a) For $e = 5$ we need to find d such that $5d \equiv 1 \pmod{\phi(65)}$ or equivalently $5d = k\phi(65) + 1 = k \cdot 4 \cdot 12 + 1 = k \cdot 48 + 1$ for an integer k. We see that $d = 29$ solves this congruence since $5d = 5 \cdot 29 = 145 = 144 + 1 = 3 \cdot 48 + 1$ and thus $5 \cdot 29 \equiv 1 \pmod{48}$.

(b) For $e = 7$ we will repeat the same process. We need to find d such that $7d \equiv 1 \pmod{\phi(65)}$ or equivalently $7d = k \cdot 48 + 1$ for an integer k. We see that $d = 7$ solves this congruence since $7d = 7 \cdot 7 = 49 = 48 + 1$ and thus $7 \cdot 7 \equiv 1 \pmod{48}$.

(c) We want to encrypt the message $P = 03$ with encryption key $e = 5$, where $n = pq = 5 \cdot 13$. We form a cyphertext block C by $E(P) = C \equiv P^e \pmod{n}$, $0 \leq C < n = 65$, i.e $3^5 \equiv 343 \equiv 48 \pmod{65}$. So that $C = 48$ is how we encrypt $P = 03$.

Question 3 Show that $1 = \sum_{d|n} \mu(d)\tau(n/d)$.

Solution Using the language of Theorem 7.16 we set $f(d) = 1$ as our arithmetic function and τ is the summatory function of f, i.e $\tau(n) = \sum_{d|n} f(d) = \sum_{d|n} 1$, which is simply the number of divisors of n. Now using the Mobius inversion formula (Theorem 7.16) we have that in fact $1 = f(n) = \sum_{d|n} \mu(d)\tau(n/d)$. And if you look at example 7.17 this is exactly the same as $1 = f(n) = \sum_{d|n} \mu(n/d)\tau(d)$.

Question 4 (Rosen 8.4.8) If RSA encryption with key $(e, n) = (5, 2881)$ produces ciphertext 0504 1874 0347 0515 2088 2356 0736 0468, what is the plaintext?

Solution Since $2881 = 43 \cdot 67$, $\phi(2881) = 42 \cdot 66 = 2772$. Since $5 \cdot 1109 \equiv 1 \pmod{2772}$, 1109 is an inverse for 5 modulo 2772. Therefore we perform the transition

$P \equiv C^{1109} \pmod{2881}$ to each 4-digit block of ciphertext. For instance $0504^{1109} \pmod{2881}$. Similarly we find 1902, 0714, 0214, 1100, 1904, 0200, and 1004 as the other blocks of the plaintext. The letters for these are EA TC HO CO LA TE CA KE.

Question 5 (Rosen 7.4.22) Compute $\prod_{d|n} \mu(d)$. Your answer should encompass three cases for n.

Solution If n is prime, then $\prod_{d|n} \mu(d) = \mu(1)\mu(n) = 1(-1) = -1$. If $s^2|n$ for some $s > 1$, then $\mu(s^2) = 0$ appears in the product, making the whole product 0. Finally, if $n = p_1 p_2 \cdots p_k, then \prod_{d|n} \mu(d) = 1 \cdot \prod_{p_i} \mu(p_i) \cdot \prod_{p_i,p_j} \mu(p_i p_j) \cdots \mu(p_1 p_2 \cdots p_k)$. The first of these products contributes k (-1)'s to the whole product. The second product contributes $\binom{k}{2}((-1)^2)$'s to the product, and in general, the ith product contributes $\binom{k}{i}((-1)^i)'s$ to the product. Therefore, we need only count the number of (-1)'s in the product, namely, $\binom{k}{1} + \binom{k}{3} + \binom{k}{5} + \cdots = 2^{k-1}$ which is even (if $k = 1$ then n is prime.) Since the product consists of an even number of (-1)'s, it must equal 1.

Question 6 List the main theorems proved in class. Indicate the method we employed to prove them.