Solutions to Quiz # 7 for Dr. Z.'s Number Theory Course for Nov. 7, 2013

1. (3 points) Using the formula, find $\phi(3003)$.

Sol. of 1: Recall that the *formula* for $\phi(n)$ is given in terms of the *prime-power decomposition* promised by the *Fundamental Theorem of Arithemetics* . You write n as

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad ,$$

and then

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) \quad .$$

We have

$$3003 = 3 \cdot 7 \cdot 11 \cdot 13 \quad ,$$

so

$$\phi(n) = 3003 \cdot (1 - \frac{1}{3})(1 - \frac{1}{7})(1 - \frac{1}{11})(1 - \frac{1}{13})$$
$$= 3 \cdot 7 \cdot 11 \cdot 13 \cdot (\frac{2}{3})(\frac{6}{7})(\frac{10}{11})(\frac{12}{13})$$
$$= 2 \cdot 6 \cdot 10 \cdot 12 = 1440 \quad .$$

Ans. to 1: $\phi(3003) = 1440$.

2. (3 points) State and prove Euler's Classical Formula for the sum-over-divisors of n of ϕ.

Solution of 2: The formula is

$$\sum_{d|n} \phi(d) = n \quad .$$

The proof goes as follows. Write *all* the fractions $\frac{i}{n}$ $i = 1, 2 \ldots, n$ (n of them), and *reduce* them, and look at the resulting denominators. The number of those fractions that have denominator n is $\phi(n)$, since this means that the numerator has no common prime divisors with the denominator n, so it must be relatively prime to n. Of course each of the denominators that show up must be divisible by n, and for every such denominator d, the number of fractions with that denominator is $\phi(d)$ (since the fractions are **reduced**, meaning there is nothing to cancel). Adding up all the possibilities, gives the identity.

3. (4 points) For the following prime p and q (let $n = pq$) public key e, and encrypted message c

(i) Check that e is an OK key, i.e. that it is coprime to $\phi(n)$.

(ii) Find the deciphering key, d, such that $de \equiv 1 \pmod{\phi(n)}$

(iii) Suppose Alice sent you the encrypted message c. Check that this is an OK message (coprime to n), and if it is find her original message?, m

$p = 3 \quad , \quad q = 5 \quad , \quad e = 5 \quad , \quad c = 7$

Sol. of 3: $n = 3 \cdot 5 = 15$, $\phi(n) = (3-1)(5-1) = 2 \cdot 4 = 8$.

(i) here $e = 5$, and since $gcd(5, 8) = 1$, the key is OK!

(ii) We need to find $d = [5^{-1}]_8$. By inspection (trying out everything from 2 to 7) we get $d = 5$ (by coincidence it is the same). We can also use the Extended Euclidean Algorithm

$$\mathbf{8} = 1 \cdot \mathbf{5} + 3$$

so $3 = \mathbf{8} - 1 \cdot \mathbf{5}$. Next

$$\mathbf{5} = 1 \cdot 3 + 2 \quad ,$$

so $2 = \mathbf{5} - 1 \cdot 3 = \mathbf{5} - 1 \cdot (\mathbf{8} - 1 \cdot \mathbf{5}) = 2 \cdot \mathbf{5} - 1 \cdot \mathbf{8}$. Next

$$3 = 1 \cdot 2 + 1 \quad ,$$

so

$$1 = 3 - 1 \cdot 2 = (\mathbf{8} - 1 \cdot \mathbf{5}) - 1 \cdot (2 \cdot \mathbf{5} - 1 \cdot \mathbf{8}) = 2 \cdot \mathbf{8} - 3 \cdot \mathbf{5} \quad ,$$

so

$$1 = 2 \cdot \mathbf{8} - 3 \cdot \mathbf{5} \quad .$$

Taking this modulo 8 we get

$$1 \equiv (-3) \cdot 5 \pmod 8$$

But $-3 \equiv 5 \pmod 8$ so

$$1 \equiv 5 \cdot 5 \pmod 8$$

and once again (the long way), we have $d = 5$.

(iii) $c = 7$, $gcd(7, 15) = 1$ so it is an OK message. To decipher it, we do

$$m \equiv c^e \pmod n \equiv 7^5 \pmod{15} \quad .$$

$$7^1 = 7 \quad , \quad 7^2 = 49 \equiv 4 \pmod{15} \quad , \quad 7^4 = 4^2 \equiv 1 \pmod{15}$$

so $7^5 \equiv 7^{1+4} = 7 \cdot 7^4 \equiv 7 \cdot 1 \equiv 7 \pmod{15}$.

Ans. to 3(iii): The original message, $m = 7$. (By coincidence it is the same!)