SPRING 2025 MATH 540: QUIZ 3

Name:

1. Define the Euler totient function $\phi(n)$ and state at least one of its properties discussed in class. (3 points)

Solution. $\phi(n)$ is the number of positive integers less than n and relatively prime to n. Equivalently, it is the number of elements in $\mathbb{Z}_n$ that have a multiplicative inverse.

The properties of $\phi(n)$ given in class are:

(i) $\phi(p) = p - 1$, for a prime p.
(ii) $\phi(ab) = \phi(a)\phi(b)$, if $\gcd(a, b) = 1$.
(iii) $\phi(p^e) = p^e - p^{e-1}$, if p is prime and $e \geq 1$.
(iv) If $n = p_1^{e_1} \cdots p_r^{e_r}$ is a prime factorization, then $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_e^{e_r-1})$.

2. Prove that if $ca \equiv cb \bmod n$ and $\gcd(c, n) = 1$, then $a \equiv b \bmod n$. (4 points)

Solution. Here are two possible solutions. For the first, write $1 = sc + tn$, for $s, t \in \mathbb{Z}$. Thus, $n \mid (1 - sc)$ showing that $sc \equiv 1 \bmod n$, i.e., c has a multiplicative inverse modulo n. Since $ca \equiv cb \bmod n$, mutliplying by c we get $sca \equiv scb \bmod n$, so $1a \equiv 1b \bmod n$, and thus $a \equiv b \bmod n$.

Alternately: We can write $ca - cb = nd$, for $d \in \mathbb{Z}$. Thus, using the equation above,

$$\begin{aligned} a &= asc + atn \\ &= s(cb + nd) + atn \\ &= scb + (sd + at)n \\ &= (1 - tn)b + (sd + at)n \\ &= b + (-tb + sd + at)n \end{aligned}$$

showing that $n \mid (a - b)$, so $a \equiv b \bmod n$.

3. Calculate $\phi(2^4 3^2 5^5 11^2)$. You can just write the formula, you needed simplify it. (3 points)

Solution. $\phi(2^4 3^2 5^5 11^2) = (2^4 - 2^3) \cdot (3^2 - 3) \cdot (5^5 - 5^4) \cdot (11^2 - 11)$.