Staff Solutions to Mini-Quiz 5

Problem 1 (6 points).

(a) What is the value of $\phi(175)$, where $\phi$ is Euler’s function?

Solution. Noting that $175 = 5^2 \cdot 7$. It follows that $\phi(175) = (5^2 - 5^1)(7 - 1) = 20 \cdot 6 = 120$. 

(b) What is the remainder of $(-12)^{482}$ divided by 175?

Solution. 144.

Since -12 and 175 are relatively prime, we have by Euler’s Theorem that $(-12)^{\phi(175)} \equiv 1 \pmod{175}$, and so

$$(-12)^{482} = ((-12)^{120})^4 \cdot (-12)^2 \equiv 1^4 \cdot (144) \equiv 144 \pmod{175}.$$ 

(c) Explain why $(-12)^{482}$ has a multiplicative inverse modulo 175.

Solution. A number has a multiplicative inverse modulo 175 iff it is relatively prime to 175. But the only prime divisors of 175 are 7 and 5, and for any $k \in \mathbb{N}$, the only prime divisors of $(-12)^k$ are the prime divisors of 12, namely 2 and 3, so $(-12)^k$ is relatively prime to 175. Alternatively, using part (b), it is enough to show that $\gcd(175, 144) = 1$, which can be verified by the Euclidean algorithm:

$$\gcd(175, 144) = \gcd(144, 31) = \gcd(31, 20) = \gcd(20, 11) = \gcd(11, 9) = \gcd(9, 2) = \gcd(2, 1) = 1.$$ 

Problem 2 (4 points).

Prove that if $k_1$ and $k_2$ are relatively prime to $n$, then so is $k_1 \cdot k_2$. (You may assume any of the results from the text or class problems. There are many ways to do this.)
Solution. ...using the Unique Factorization Theorem.

By Unique Factorization, the prime divisors of \( k_1 \cdot k_2 \) are the same as the prime divisors of \( k_1 \) along with the prime divisors of \( k_2 \). If \( k_1 \) and \( k_2 \) are relatively prime to \( n \), they have no prime divisors in common with \( n \), so neither does \( k_1 k_2 \), that is, \( k_1 k_2 \) is relatively prime to \( n \).

...using the fact that \( k \) is relatively prime to \( n \) iff \( k \) has an inverse modulo \( n \).

If \( j_1 \) is an inverse of \( k_1 \) modulo \( n \), that is

\[
j_1 k_1 \equiv 1 \pmod{n},
\]

and likewise \( j_2 \) is an inverse of \( k_2 \), then it follows immediately that

\[
(j_2 j_1)(k_1 k_2) \equiv 1 \pmod{n}.
\]

That is, \( k_1 k_2 \) also has an inverse. Since we know that \( k_1 k_2 \equiv k_1 \cdot n k_2 \pmod{n} \), any inverse of \( k_1 k_2 \) will also be an inverse of \( k_1 \cdot n k_2 \).

...using the fact that \( k \) is relatively prime to \( n \) iff \( k \) is cancellable modulo \( n \).

If \( k_1 \) and \( k_2 \) are cancellable modulo \( n \), then you can cancel \( k_1 k_2 \) by first cancelling \( k_1 \) and then cancelling \( k_2 \). \( \blacksquare \)