Session 3: Euler's Totient Function

Discuss modular multiplicative inverses with students:

Get them to explore the conditions for an inverse to exist in modular terms by considering different examples.

i.e. For an integer 'a' modulus 'm',

$a^{-1} \equiv x \pmod{m}$ where x is an integer.

$aa^{-1} \equiv ax \equiv 1 \pmod{m}$

Students need to select different values of a and m and explore when the inverse exists. They should determine that it exists iff (if and only if) a and m are co-prime.

Show students Euler's Totient function. Get them to explore this for the numbers 1 to 30.

Show students Euler's Function (providing 'a' is coprime to 'n') :

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Get students to explore this relationship.

Show students this method for finding the last digit of a large power:

The theorem may be used to easily reduce large powers modulo *n*. For example, consider finding the last decimal digit of 7^{222}, i.e. $7^{222} \pmod{10}$. Note that 7 and 10 are coprime, and $\phi(10) = 4$. So Euler's theorem yields $7^4 \equiv 1 \pmod{10}$, and we get $7^{222} \equiv 7^{4\times55+2} \equiv (7^4)^{55}\times7^2 \equiv 1^{55}\times7^2 \equiv 49 \equiv 9 \pmod{10}$.