Modular Arithmetic

- *a = b mod (m)* means that when *a* is divided by *m* the remainder is *b*.
- Examples
- 11 = 1 mod (5)
- 20 = 2 mod (6)

Modular Inverse

- Another aspect of modular math is the concept of a modular inverse.
- Two numbers are the modular inverses of each other if their product equals 1.
- For instance, 7 * 343 = 2401, but if our modulus is 2400, the result is:
- (7 * 343) mod 2400 = 2401 – 2400 = 1 mod 2400

Exponentiation

- **Exponentiation** is taking numbers to powers, such as 2^3, which is 2 * 2 * 2 = 8. In this example, 2 is known as the **base** and 3 is the **exponent**. There are some useful algebraic identities in exponentiation.
- $(b^x) * (b^y) = b^{x+y}$
- $(b^x)^y = b^{xy}$

Exponential Period modulo *n*

- Euler noticed that $\varphi(n)$ was the "exponential period" modulo n for numbers relatively prime with n.
- What that means is that for any number $a < n$, if a is relatively prime with n, $a^{\varphi(n)} \bmod n = 1$.
- So if you multiply a by itself $\varphi(n)$ times, modulo n, the result is 1. Then if you multiply by a one more time, you are finding the product of $1 * a$ which is a, so you are starting over again.
- Hence, $a^{\varphi(n)} * a = a^{\varphi(n)+1} \bmod n = a$.

Exponential Period modulo *n*

- For example, if n is 5 (a prime number), then $\varphi(5) = 4$. Let a be 3 and compute
- $a^{\varphi(n)} \bmod n = 3^4 = 3 * 3 * 3 * 3 \bmod 5$