Modular Arithmetic Facts

1. We say that $x \equiv y \pmod{n}$ if x and y has the same remainder when divided by n; another way to put it is to say that n divides $x - y$.

2. Congruence classes can be added and multiplied the same way as normal numbers: for example, if

$$\begin{aligned} x &\equiv 1 \pmod{n} \\ y &\equiv 2 \pmod{n} \end{aligned}$$

then we have that $x + y \equiv 3 \pmod{n}$, $xy \equiv 2 \pmod{n}$.

3. There's no division with congruence classes! However, if a and n are coprime (that is, have no factors in common), then there exists a unique congruence class a^{-1} such that

$$aa^{-1} \equiv 1 \pmod{n}$$

For example, $4 \equiv 2^{-1} \pmod{7}$ because $2 \cdot 4 \equiv 1 \pmod{7}$.

4. **Fermat's Little Theorem:** If p is prime, and a isn't divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

5. **Euler's Theorem:** This is a generalization of Fermat's little theorem. If the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then define the Euler phi function as:

$$\phi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$$

For example, if $n = 12$, then $n = 2^2 \cdot 3^1$, and therefore

$$\phi(12) = (2^2 - 2^1) \cdot (3^1 - 3^0) = 2 \cdot 2 = 4$$

Euler's theorem states that if a and n are coprime (have no factors in common), then

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

Note: The Euler phi function actually counts the number of integers in the set $\{1, 2, \ldots, n\}$ that are coprime to n. For example, $\phi(12) = 4$ because the only integers in $\{1, 2, \ldots, 12\}$ coprime to 12 are $1, 5, 7$ and 11.