Math 406 Section 6.1: Inverses, Wilson's Theorem and Fermat's Little Theorem

1. **Inverses:** Notice that $2 \cdot 3 \equiv 1 \bmod 5$. We say that 2 and 3 are (multiplicative) inverses of one another mod 5. Similarly $3 \cdot 3 \equiv 1 \bmod 8$ so 3 is its own inverse mod 8.

   Existence of Inverses: For a modulus m the integer a has an inverse iff $\gcd(a, m) = 1$.

   Proof

   Well, a has an inverse iff $ax \equiv 1 \bmod m$ has a solution which will only occur if $\gcd(a, m) = 1$. Note that this inverse is unique mod m because there will be only one solution. $\mathcal{QED}$

   Example: If $m = 20$ then $a = 1, 3, 7, 9, 11, 13, 17, 19$ have inverses. In fact $1, 9, 11, 19$ are their own inverses $3, 7$ are inverses of one another and $13, 17$ are inverses of one another:

   $$1 \cdot 1 \equiv 9 \cdot 9 \equiv 11 \cdot 11 \equiv 19 \cdot 19 \equiv 3 \cdot 7 \equiv 13 \cdot 17 \equiv 1 \bmod 20$$

   Inverses mod primes: For a prime modulus p every one of $1, ..., p-1$ has an inverse and 1 and $p-1$ are the only two which are their own inverses.

   Proof: The first follows because all of $1, ..., p-1$ are coprime to p and the second was proved on a homework. More specifically if $a^2 \equiv 1 \bmod p$ then $a \equiv \pm 1 \bmod p$. $\mathcal{QED}$

2. **Wilson's Theorem:** If p is prime then $(p-1)! \equiv -1 \bmod p$.

   Proof:

   The case where $p = 2$ is trivial to show so let's look at primes $p \geq 3$.

   Consider the numbers $1, 2, 3, ..., p-1$. We've seen that 1 and $p-1$ are their own inverses and all of $2, ..., p-2$ pair up as inverses.

   $$(p-1)! = 1 \cdot \underbrace{2 \cdot 3 \cdot ... \cdot (p-2)}_{\text{Pair as inverses}} \cdot (p-1) \equiv 1 \cdot (\text{products of 1s}) \cdot (p-1) \equiv -1 \bmod p$$

   $\mathcal{QED}$

   Wilson's Theorem can be used to simply other factorials.

   Example: To find the least nonnegative residie of 20! mod 23 note that:

   $$\begin{aligned} 22! &\equiv -1 \bmod 23 \\ (22)(21)20! &\equiv -1 \bmod 23 \\ (-1)(-2)20! &\equiv -1 \bmod 23 \\ (-1)(-1)(-2)20! &\equiv (-1)(-1) \bmod 23 \\ (-2)20! &\equiv 1 \bmod 23 \\ (-12)(-2)20! &\equiv (-12) \bmod 23 \\ 20! &\equiv 11 \bmod 23 \end{aligned}$$

3. **Fermat's Little Theorem:** If p is a prime and $a \in \mathbb{Z}$ with $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

   Proof:

   The set $\{0, 1, 2, 3, ..., p-1\}$ is a complete set of residues mod p. Since $p \nmid a$ we know $\gcd(a, p) = 1$ and so (by an earlier theorem) the set $\{0, a, 2a, 3a, ..., (p-1)a\}$ is also a complete set of residues mod p.

   There is then a 1-1 matching of these via congruence mod p. Since the 0s are congruent to one another, the remaining values must be congruent in some order. We don't know what the order is but we do know that if we multiply the remaining values we will get the same result mod p:

$$\begin{aligned} a \cdot 2a \cdot ... \cdot (p-1)a &\equiv 1 \cdot 2 \cdot ... \cdot (p-1) \bmod p \\ a^{p-1} \cdot 1 \cdot 2 \cdot ... \cdot (p-1) &\equiv 1 \cdot 2 \cdot ... \cdot (p-1) \bmod p \\ a^{p-1} &\equiv 1 \bmod p \end{aligned}$$

   Notice that we can cancel all of the $1, 2, ..., p-1$ without affecting the modulus because they are coprime to p. $\mathcal{QED}$

   Example: Suppose we wanted the least nonnegative residue of 5^{123} mod 13. Since $13 \nmid 5$ we have $5^{12} \equiv 1 \bmod 13$ and so

$$5^{123} \equiv 5^{12(10)+3} \equiv (5^{12})^{10} 5^3 \equiv (1)^{10} 5^3 \equiv 5^3 \equiv 125 \equiv 8 \bmod 5$$

   Theorem: If p is a prime and $a \in \mathbb{Z}$ then $a^p \equiv a \bmod p$.
   Proof: If $p \nmid a$ then we take FLiT and multiply both sides by a. If $p \mid a$ then both sides are 0 mod p and the result follows. $\mathcal{QED}$