Week 8 List of Theorems

Linear Congruence Theorem 1 (LCT 1)
Let $\gcd(a, m) = d \geq 1$. The linear congruence $ax \equiv c \pmod{m}$ has a solution if and only if $d \mid c$.
Moreover, if x_0 is one solution, then the complete solution is $x \equiv x_0 \pmod{\frac{m}{d}}$.
Equivalently, $x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod{m}$.

Linear Congruence Theorem 2 (LCT 2)
Let $\gcd(a, m) = d \geq 1$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x_0]$ is one solution, then the complete solution in $\mathbb{Z}_m$ is

$$\left\{[x_0], [x_0 + \frac{m}{d}], \cdots, [x_0 + (d-1)\frac{m}{d}]\right\}.$$

Existence of Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)
Let p be a prime number. If $[a]$ is any non-zero element in $\mathbb{Z}_p$, then $[a]^{-1}$ exists.

Fermat's Little Theorem (FℓT)
Let $a \in \mathbb{Z}$. If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary to Fermat's Little Theorem
For any integer a and any prime p, $a^p \equiv a \pmod{p}$.

Chinese Remainder Theorem (CRT)
If $\gcd(m_1, m_2) = 1$, then for any choice of $a_1, a_2 \in \mathbb{Z}$, there exists a solution to the simultaneous congruences

$$\begin{array}{rcll} n & \equiv & a_1 & \pmod{m_1} \\ n & \equiv & a_2 & \pmod{m_2}. \end{array}$$

Moreover, if n_0 is one solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2}$.

Splitting the Modulus (SM)
Let m_1 and m_2 be coprime positive integers. Then for any two integers x and a,

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases} \text{(simultaneously)} \iff x \equiv a \pmod{m_1 m_2}.$$