Week 7 List of Theorems

Linear Diophantine Equation Theorem Part 1 (LDET 1)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a, b)$. The linear Diophantine equation $ax + by = c$ has an integer solution if and only if $d \mid c$.

Linear Diophantine Equation Theorem Part 2 (LDET 2)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a, b) \neq 0$. If (x_0, y_0) is one particular integer solution to $ax + by = c$, then the complete set of integer solutions is

$$\left\{ \left(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n \right) \;\middle|\; n \in \mathbb{Z} \right\}.$$

Congruence is an Equivalence Relation (CER))
Let $m \in \mathbb{N}$, and $a, b, c \in \mathbb{Z}$. Then each of the following statements are true.

1. $a \equiv a \pmod{m}$.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Properties of Congruence (PC)
If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

1. $a + b \equiv a' + b' \pmod{m}$;
2. $a - b \equiv a' - b' \pmod{m}$; and
3. $a \cdot b \equiv a' \cdot b' \pmod{m}$.

Divisibility Rules [Optional]
A positive integer n is divisible by...

a) 2^k if and only if the last k digits are divisible by 2^k.

b) 3 (or 9) if and only if the sum of the digits is divisible by 3 (or 9).

c) 5^k if and only if the last k digits are divisible by 5^k.

d) 7 (or 11 or 13) if and only if the alternating sum of triples of digits is divisible by 7 (or 11 or 13). For example

$$7 \mid 123456789 \qquad \Leftrightarrow \qquad 7 \mid (789 - 456 + 123)$$

e) 11 if and only if the alternating sum of digits is divisible by 11.

Congruences and Division (CD)
If $ac \equiv bc \pmod{m}$ and $\gcd(m, c) = 1$, then $a \equiv b \pmod{m}$.

Congruent Iff Same Remainder (CISR)
Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Then $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

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, $x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod{m}$.