TYPE YOUR NAME HERE
HW 19: 3.27-3.29
M328K
April 3th, 2012

3.27 Theorem. *Let a, b, m, and n be integers with $m > 0$ and $n > 0$. Then the system*

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

has a solution if and only if $(n, m)|a - b$.

Proof. Let a, b, m, and n be integers with $m > 0$ and $n > 0$.

First assume that the system

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

has a solution x. So by definition of congruence mod n we have $n \mid x-a$ and $m \mid x-b$. And since (n, m) divides both n and m, we have $(n, m) \mid x - a$ and $(n, m) \mid x - b$. Therefore by theorem 1.2 $(n, m) \mid x - b - (x - a)$, or $(n, m) \mid a - b$.

Now assume that $(n, m) \mid a - b$.

□

3.28 Theorem. *Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m, n) = 1$. Then the system*

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

has a unique solution modulo mn.

Proof. Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m, n) = 1$. Since $1 \mid a - b$, then by theorem 3.27 there must be a solution to the system

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

Let x_0 be a solution to this system. Let x_0' be the integer such that $x_0 \equiv x_0' \pmod{mn}$.

□

3.29 Theorem (Chinese Remainder Theorem)**.** *Suppose* $n_1, n_2, \ldots, n_L$ *are positive integers that are pairwise relatively prime, that is,* $(n_i, n_j) = 1$ *for* $i \neq j$, $1 \leq i, j \leq L$. *Then the system of* L *congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product $n_1 n_2 n_3 \cdots n_L$.

Proof. Type your proof here! □