

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*

$$\begin{aligned}x &\equiv a \pmod{n} \\x &\equiv b \pmod{m}\end{aligned}$$

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

Proof. Type your proof here!

□

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

$$\begin{aligned}x &\equiv a \pmod{n} \\x &\equiv b \pmod{m}\end{aligned}$$

has a unique solution modulo mn .

Proof. Type your proof here!

□

3.29 Theorem (Chinese Remainder Theorem). *Suppose n_1, n_2, \dots, 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!

□