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

First assume that the system

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

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 $(n, m) \mid a-b$. Let j and k be integers such that $jn+km = (n, m)$. //TODO: finish □

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. 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

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

Let x_0 be any solution to this system. Let x_0' be the integer in the canonical complete residue system mn such that $x_0 \equiv x_0' \pmod{mn}$. Let x_1 be any other solution to the system. Let x_1' be the integer in the canonical complete residue system mn such that $x_1 \equiv x_1' \pmod{mn}$. We will show that $x_0' = x_1'$.

Since x_0 and x_1 are both solutions to the system of equations, we know that $n \mid x_0 - a$ and $n \mid x_1 - a$, so by theorem 1.2 $n \mid (x_0 - a) - (x_1 - a)$ or $n \mid x_0 - x_1$. Similarly, $m \mid x_0 - x_1$. By theorem 1.42, this means that $nm \mid x_0 - x_1$. By the definition of congruence mod n, $x_0 \equiv x_1 \pmod{nm}$. So by theorem 1.11 $x_0 \equiv x_1' \pmod{nm}$. And because $x_0'0$ and x_1' are members of the canonical complete residue system mod mn, and x_0 is congruent to both of them modulo mn, it must be that $x_0' = x_1'$. □

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. Suppose $n_1, n_2, \ldots, n_L$ are positive integers that are pairwise relatively prime. We will show by induction that the system 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 $n_1 n_2 \cdots n_L$. As our basecase, suppose $L = 2$. In this case, because $(n_1, n_2) = 1$, theorem 3.28 says that there is a unique solution to the system of equations modulo $n_1 n_2$. As our induction hypothesis, assume that there exists some $k \geq 2$ such that a system of k equations will have x', a unique solution modulo $n_1 n_2 \cdots n_k$. Since all the n's are pairwise coprime, then by lemma 1 $(n_{k+1}, n_1 n_2 \cdots n_k) = 1$. //TODO: show that a solution x_0 to $k+1$ equations exists. Let x_1 be any other solution to the system of $k+1$ equations. For each integer i from 1 to $k+1$, because $x_0 \equiv a_i \pmod{n_i}$ and $x_1 \equiv a_i \pmod{n_i}$, by theorem 1.11 $x_0 \equiv x_1 \pmod{n_i}$ and $n_i \mid x_0 - x_1$. For convienence, let $s = n_1 n_2 \cdots n_{k+1}$. So by lemma 2 $s \mid x_0 - x_1$ and $x_0 \equiv x_1 \pmod{s}$. Let x_0' and x_1' be elements of the canonical complete residue set modulo s such that $x_0 \equiv x_0' \pmod{s}$ and $x_1 \equiv x_1' \pmod{s}$. By theorem 1.11 $x_0 \equiv x_1' \pmod{s}$. Therefore $x_0' = x_1'$ and there is exactly one solution to the system of equations modulo s.

Lemma 1: Let p be an integer and $n_1, n_2, \ldots, n_m$ be integers which are pairwise relativily prime. Also, let p be coprime with every n_i. We will show that $(p, n_1 n_2 \cdots n_m) = 1$. This will be a proof by induction. As a base case, let $m = 1$. So $(p, n_1) = 1$ by definition. Our induction hypothesis is that there exists some $k \geq 1$ such that $(p, n_1 n_2 \cdots n_k) = 1$. By definition, $(p, n_{k+1}) = 1$, so by theorem 1.43 $(p, n_1 n_2 \cdots n_{k+1}) = 1$.

Lemma 2: Let $n_1, n_2, \ldots, n_m$ be integers which are pairwise relativley prime. Let x and y be integers with $n_i \mid x - y$ for each n_i. We will show by induction that $n_1 n_2 \cdots n_m \mid x - y$. As our base case, if $m = 1$, then $n_1 \mid x - y$ by definition. Our induction hypothesis is that there exists an integer $k \geq 1$ such that $n_1 n_2 \cdots n_k \mid x - y$. Since $n_{k+1} \mid x - y$, then by theorem 1.42 $n_1 n_2 \cdots n_{k+1} \mid x - y$. $\square$