Geoffrey Parker - grp352
HW 20: 4.1 - 4.6
M328K
April 5th, 2012

4.1 Exercise. *For $i = 0, 1, 2, 3, 4, 5,$ and 6, find the number in the canonical complete residue system to which 2^i is congruent modulo 7. In other words, compute $2^0 \pmod 7, 2^1 \pmod 7, 2^2 \pmod 7, \ldots, 2^6 \pmod 7$.*

Solution.

$$
\begin{aligned}
2^0 &\pmod 7 = 1\\
2^1 &\pmod 7 = 2\\
2^2 &\pmod 7 = 4\\
2^3 &\pmod 7 = 1\\
2^4 &\pmod 7 = 2\\
2^5 &\pmod 7 = 4\\
2^6 &\pmod 7 = 1
\end{aligned}
$$

□

4.2 Theorem. *Let a and n be natural numbers with $(a, n) = 1$. Then $(a^j, n) = 1$ for any natural number j.*

Proof. Let a and n be natural numbers with $(a, n) = 1$ We will show by induction that $(a^j, n) = 1$ for any natural number j. As a base case, consider $j = 1$. In this case, $(a^j, n) = 1$ is simply $(a, n) = 1$, which is given. Our inductive hypothesis is that there exists some natural number $k < j$ such that $(a^k, n) = 1$. For our inductive step, since $(a^k, n) = 1$ and $(a, n) = 1$, then by theorem 1.43 $(a^{k+1}, n) = 1$.

□

4.3 Theorem. *Let a, b, and n be integers with $n > 0$ and $(a, n) = 1$. If $a \equiv b \pmod{n}$, then $(b, n) = 1$.*

Proof. Let a, b, and n be integers with $n > 0$, $(a, n) = 1$, and $a \equiv b \pmod{n}$. We will show that $(b, n) = 1$. Using the definitions of divides and congruence, we can say that:

$$n \mid a - b$$

$$nm = a - b$$

$$a = mn + b$$

for some integer m. Because $n \neq 0$, we can say by theorem 1.33 that $(a, n) = (b, n)$. Therefore $(b, n) = 1$. $\square$

4.4 Theorem. *Let a and n be natural numbers. Then there exist natural numbers i and j, with $i \neq j$, such that $a^i \equiv a^j \pmod{n}$.*

Proof. Let a and n be natural numbers. The definition of complete residue systems says that every natural number x is congruent modulo n to exactly one element of the canonical complete residue system modulo n, which has n elements. Consider the set of integers $S = \{a^1, a^2, \ldots a^{n+1}\}$. Since S has $n + 1$ elements and each element is congruent to exactly one element of the canonical complete residue system modulo n, then by the pigeonhole principle there must be two elements of S, call them a^i and a^j, which are congruent modulo n to the same element of the residue system, call it x. And since $a^i \equiv x \pmod{n}$ and $a^j \equiv x \pmod{n}$, by theorem 1.11 $a^i \equiv a^j \pmod{n}$. $\square$

4.5 Theorem. *Let a, b, c, and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and $(c, n) = 1$, then $a \equiv b \pmod{n}$.*

Proof. Let a, b, c, and n be integers with $n > 0$, $ac \equiv bc \pmod{n}$, and $(c, n) = 1$. By the definition of congruence:

$$n \mid ac - bc$$

$$n \mid c(a - b)$$

and since $(c, n) = 1$, by theorem 1.41 $n \mid a - b$. Therefore by the definition of congruence $a \equiv b \pmod{n}$.

Also, this is just theorem 1.45 again. $\square$

4.6 Theorem. *Let a and n be natural numbers with $(a, n) = 1$. Then there exists a natural number k such that $a^k \equiv 1 \pmod{n}$.*

Proof. Let a and n be natural numbers with $(a, n) = 1$.

$n \mid a^k - 1$

$\square$

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 $n_1 n_2 \cdots n_k$.

Consider the system of congruences

$$y \equiv x' \pmod{n_1 n_2 \cdots n_k}$$

$$y \equiv a_{k+1} \pmod{n_{k+1}}$$

Since all the n's are pairwise coprime, then by lemma 1 $(n_{k+1}, n_1 n_2 \cdots n_k) = 1$. Therefore by theorem 3.28 the solution y exists. And because $y \equiv x' \pmod{n_1 n_2 \cdots n_k}$, y is a solution to the first k congruences.

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 $(p, n_1 n_2 \cdots n_{k+1}) = 1$.

□