

Assignment 1: Selected Solutions

Section 1.3

10. Let a, b , and n be integers. Prove that if $a \equiv b \pmod{n}$ then $(a, n) = (b, n)$.

Proof: Recall the set $I = \{xa + yn \mid x, y \in \mathbb{Z}\} = (a, n)\mathbb{Z}$. Now, since $a \equiv b \pmod{n}$, $n \mid (b - a)$. Therefore, $b - a = nk$ for some $k \in \mathbb{Z}$. Equivalently, $b = a + nk \in I$. It follows that $(a, n) \mid b$. Since also $(a, n) \mid n$, it follows from the definition of *greatest common divisors* that $(a, n) \mid (b, n)$. By repeating the argument, with the roles of a and b reversed, we conclude that $(b, n) \mid (a, n)$. Hence, they are equal. ■

26. Let p be a prime number and $a, b \in \mathbb{Z}$. Prove that $(a + b)^p \equiv a^p + b^p \pmod{p}$.

Proof: Using the binomial theorem we may write

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i.$$

Note that $\binom{p}{0} = \binom{p}{p} = 1$. We claim that, for $1 \leq i \leq p - 1$, $p \mid \binom{p}{i}$. Indeed,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \in \mathbb{Z}.$$

This implies that $i!(p-i)! \mid p(p-1)!$. Since $i < p$, $i! \nmid p$, and since $i > 0$, $(p-i)! \nmid p$. Thus, $i!(p-i)! \mid (p-1)!$. It follows that $p \mid \binom{p}{i}$, and, therefore

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

■

Section 1.4

27. Prove Wilson's theorem, which states that if p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

Proof: Consider the product $[1][2] \cdots [p-2][p-1] \in \mathbb{Z}_p^\times$. Observe that if $[n] = [n]^{-1}$, then $n^2 \equiv 1 \pmod{p}$. Thus, $p \mid (n^2 - 1)$. It follows that $p \mid (n+1)$ or $p \mid (n-1)$, so $[n] = [\pm 1]$. By pairing each element in the product $[2], \dots, [p-2]$ with its inverse, we conclude that the product

$$[2] \cdots [p-2] = [1] \in \mathbb{Z}_p^\times.$$

Thus, $[1][2] \cdots [p-2][p-1] = [1][1][p-1] = [-1] \in \mathbb{Z}_p^\times$ and the result follows. ■

Section 2.1

11. Let k and n be positive integers. Fix $m \in \mathbb{Z}$ and define $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_k$ by $f([x]_n) = [mx]_k$. Show that f defines a function if, and only if, $k \mid mn$.

Proof: First, if $k \nmid mn$, then

$$f([n]_n) = [mn]_k \neq [0]_k = f([0]_n).$$

Hence, f is not well-defined. On the other hand, assume $k \mid mn$ and $[x]_n = [y]_n$. Then, $n \mid (x - y)$, and $k \mid nm \mid (mx - my)$. Thus,

$$f([x]_n) = [mx]_k = [my]_k = f([y]_n)$$

and f is well-defined. ■

20. Define $f : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([x]_{mn}) = ([x]_m, [x]_n)$. Show that f is surjective if, and only if $(m, n) = 1$.

Proof: Note that both \mathbb{Z}_{mn} and $\mathbb{Z}_m \times \mathbb{Z}_n$ are sets of size mn . Hence, f is surjective if, and only if, it is injective. It is, therefore, enough to prove that f is injective if, and only if, $(m, n) = 1$.

First, assume that $(m, n) = 1$ and $f([x]_{mn}) = f([y]_{mn})$. Then, $m|(x-y)$ and $n|(x-y)$. It follows that $[m, n](x-y)$. But, $[m, n] = \frac{mn}{(m, n)} = mn$, so $[x]_{mn} = [y]_{mn}$.

Now, assume that $(m, n) = d > 1$. Write $m = kd$ and $n = dh$. Then, $f([kdh]_{mn}) = ([kdh]_m, [kdh]_n) = ([mh]_m, [kn]_n) = ([0]_m, [0]_n)$. However, $mn \nmid [m, n] = kdh$, so $[kdh]_{mn} \neq [0]_{mn}$. ■