MATH 113: DISCRETE STRUCTURES
HOMEWORK DUE FRIDAY WEEK 11

Problem 1. Use the Fundamental Theorem of Arithmetic to prove that if p is prime, a and b are integers, and $p|ab$, then either $p|a$ or $p|b$ (or both).

Problem 2. Let p be a prime and let a be an integer $1 \leq a \leq p-1$. Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$. Use the division algorithm to write

$$ia = pq_i + r_i$$

with $0 \leq r_i < p$ and integers q_i for $1 \leq i \leq p-1$.

(a) Prove that $r_i > 0$ for each i.
(b) If $r_i = r_j$, show that $p|(i-j)a$, and explain why we can then conclude that $i = j$.
(c) Prove that $\{r_1, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}$.

Problem 1. Use the Fundamental Theorem of Arithmetic to prove that if p is prime, a and b are integers, and $p|ab$, then either $p|a$ or $p|b$ (or both).

First note, using the Fundamental Theorem

$$ab = pm$$

$$\left(p_1^{a_1} \cdots p_n^{a_n}\right)\left(p_1^{b_1} \cdots p_n^{b_n}\right) = p\left(p_1^{m_1} \cdots p_n^{m_n}\right)$$

$$\left(p_1^{a_1+b_1-m_1} \cdots p_n^{a_n+b_n-m_n}\right) = p$$

$\Rightarrow$ $a_i + b_i - m_i = 0$ for all but one i,
in which case, WLOG let this case be 1 so $p_1 = p$
$a_1 + b_1 - m_1 = 1$

$\Rightarrow$ $a_i = m_i - b_i$
Using these $b_i = m_i - a_i$

we see

$$\left(p_1^{a_1} \cdots p_n^{a_n}\right) = p\left(p_1^{m_1 - b_1} \cdots p_n^{m_n - b_n}\right)$$

$\Rightarrow$ $a = pq$

$$\left(p_1^{b_1} \cdots p_n^{b_n}\right) = p\left(p_1^{m_1 - a_1} \cdots p_n^{m_n - a_n}\right)$$

$\Rightarrow$ $b = pr$.

w/ one issue if a_1 or b_1 is 0.
if this is true then $m_1 - b_1$ or $m_1 - a_1$ is -1 respectively.
WLOG, let $a_1 = 0$, if so then we know $p \nmid a$, however, $b_1 = m_1 - a_1 + 1 = m_1 + 1$, thus the second equality holds & $p | b$. Lastly, if $a_1 = b_1 = 0$, then we know $p \nmid ab$.

If $a_i, b_i > 0$, then we see $p \nmid a$ & $p \nmid b$.

thus if $p | ab \Rightarrow p | a$ or/and $p | b$

2. a. Suppose otherwise, then for 0, this would mean that ia is a multiple of p, i.e. $p | ia$. But $1 \leq i \leq p-1$ and $1 \leq a \leq p-1$, thus ia cannot be a multiple of p, since it would contradict the primality of p because, as shown in 1 if $p | ia \Rightarrow p | i$ or $p | a$, but there does not exist an integer m or n such that

$$a = pm$$
$$i = pn$$

Since $a, i < p$. Thus $r_i > 0$

b. Let

$$ia = pq_i + r_i$$
$$- \quad ja = pq_j + r_j$$
$$(i-j)a = p(q_i - q_j)$$

$p | (i-j)a$ w/ $m = q_i - q_j$

we know $p \nmid a$ and $p \nmid (i-j)$ since $1 \leq a \leq p-1$ and $0 \leq (i-j) < p$, thus one must be zero, but a is nonzero, thus $i - j = 0 \Rightarrow i = j$

c. We know that $|\{r_1, \dots, r_{p-1}\}| = p-1$, and we know that (by b.) that is $r_i = r_j \Rightarrow i = j$, meaning that each r_i is distinct and that each $r_i > 0$ (a.). Thus, since we know $r_i < p$, the only option is that each r_i corresponds to an element in $\{1, 2, \dots, p-1\}$

or, $\{r_1, r_2, \dots, r_{p-1}\} = \{1, 2, \dots, p-1\}$