due Feb 7 | Homework Set 4 (sections 1.3, 2.1 – 2.2) | Name: _____

1. Let a and b be integers. Prove that $\gcd(a, b) = 1$ if and only if there does not exist any prime p such that p divides a and p divides b.

Let a and b be integers. Suppose there exists an integer c such that c divides a and c divides b. We may assume $c \geq 1$. By Corollary 1.4, c divides gcd(a,b).

($\Rightarrow$) Assume that gcd(a,b) = 1.
Then c divides 1. Hence, $c = \pm 1$. By definition, c is not prime. Thus, there is no such prime.

($\Leftarrow$) Assume that gcd(a,b) $\neq 1$.
Then there exists some integer $d > 1$ such that $d = \gcd(a,b)$. By Theorem 1.10, d is a product of primes. Thus, there is a prime p such that p divides d. By transitivity, p divides both a and b. Thus, we have shown by proof by contrapositive that if no prime divides both a and b then the gcd(a,b) = 1.

2. Let a and b be integers with n and k positive integers. Prove that if $a \equiv b \mod n$ and k divides n, then $a \equiv b \mod k$.

Let n and k be positive integers such that k divides n.
Let a and b be integers integers such that $a \equiv b \mod n$.
By definition, n divides (a-b). Thus, there exists an integer f such that $(a-b) = nf$. Also, since k divides n, there exists an integer g such that $n = kg$. Combining these, we have $(a-b) = nf = (kg)f = k(gf)$. Thus, k divides (a-b). Then by definition, $a \equiv b \mod k$.

3. Prove part (8) of Theorem 2.7:
For any classes $[a]$, $[b]$, and $[c]$ in $\mathbb{Z}_n$, prove $([a] \oplus [b]) \odot [c] = ([a] \odot [c]) \oplus ([b] \odot [c])$.

Suppose [a], [b], and [c] are classes in $\mathbb{Z}_n$ for some $n \geq 2$.
Then using the definition of addition and multiplication in $\mathbb{Z}_n$ and the distributive rules in $\mathbb{Z}$, we have

$$([a] \oplus [b]) \odot [c] = [a+b] \odot [c] = [(a+b)c]$$
$$= [ac + bc] = [ac] \oplus [bc] = ([a] \odot [c]) \oplus ([b] \odot [c]).$$

4. Answer the following questions:
   a. If $r \equiv 4 \, mod \, 10$ and $s \equiv -3 \, mod \, 10$, then what is $2r + 3s$ congruent to modulo 10?

Using congruencies given above, we get that

$2r + 3s \equiv 2(4) + 3(-3) \bmod 10 = -1 \bmod 10 \equiv 9 \bmod 10.$

   b. Show that $a^{p-1} \equiv 1 \, mod \, p$ for $p = 5$ and $a = 2$

For $p = 5$ and $a = 2$, we have that

$a^{p-1} = 2^{5-1} = 16 = 1 + 5(3) \equiv 1 \bmod 5 \equiv 1 \bmod p.$

5. Find all of the solutions of each congruence:
   a. $3x \equiv 1 \, mod \, 7$

The only solution is $x \equiv 5 \bmod 7$.

x	3x-1
0	-1
1	2
2	5
3	8
4	11
5	14
6	17

   b. $6x \equiv 9 \, mod \, 15$

The solutions are $x \equiv 4 \bmod 15$, $x \equiv 9 \bmod 15$, and $x \equiv 14 \bmod 15$.

6. Write out the addition and multiplication tables for $\mathbb{Z}_5$. Find an element of $\mathbb{Z}_5$ such that every non-zero element of $\mathbb{Z}_5$ is a positive power of that element.

⊕	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

⊙	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]