CSE 311: Foundations of Computing I

Section 4: Number Theory

1. Conceptual Review

(a) What's the definition of "a divides b"?

(b) What's the definition of "a is congruent to b modulo m"?

(c) What's the Division Theorem?

2. Modular Computation

(a) Circle the statements below that are true.
Recall for $a, b \in \mathbb{Z}$: $a|b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$.

(a) $1|3$
(b) $3|1$
(c) $2|2018$
(d) $-2|12$
(e) $1 \cdot 2 \cdot 3 \cdot 4|1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

(b) Circle the statements below that are true.
Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv b \pmod{m}$ iff $m|(a - b)$.

(a) $-3 \equiv 3 \pmod{3}$
(b) $0 \equiv 9000 \pmod{9}$
(c) $44 \equiv 13 \pmod{7}$
(d) $-58 \equiv 707 \pmod{5}$
(e) $58 \equiv 707 \pmod{5}$

3. Divisibility Proof

Prove that for all integers n, d, if $d \mid n$, then $-d \mid n$.

4. Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv_m b$, where a and b are integers, then $a \equiv_n b$.

5. GCD

Compute the following using the Euclidean algorithm. Show your intermediate results as a sequence of gcd() calls.

(a) $\gcd(9, 6)$

(b) $\gcd(18, 14)$

(c) $\gcd(80, 44)$

(d) $\gcd(77, 43)$

6. Modular Proof

Prove from definitions that for integers a, b, c, d and positive integer m, if $a \equiv_m b$ and $c \equiv_m d$, then $a - c \equiv_m b - d$.

7. A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.