Section 04: Number Theory

1. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Calculate gcd(9,6)

(d) Calculate gcd(18,14)

(e) Calculate gcd(80,44)

(f) Calculate gcd(77,43)

(g) Find the multiplicative inverse of $6 \pmod 7$.

(h) Does 49 have an multiplicative inverse $\pmod 7$?

2. Modular Computation

(a) Circle the statements below that are true.
Recall that 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 if $a|b$ and $b|a$, where a and b are integers, then $a = b$ or $a = -b$.

4. Another Divisibility Proof

Prove that if $n|m$, and n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

5. Modular Proof

Prove from the definitions that for integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$

6. 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.

7. Extended Euclidean Algorithm Application: Multiplicative Inverse

Note: You are not responsible for knowing how to run the Extended Euclidean Algorithm. You are responsible for knowing what it is used for.

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2 (\text{mod } 33)$ for all of its integer solutions z.