CSE 311: Foundations of Computing I

Section 4: Number Theory Solutions

1. Conceptual Review

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

Solution:

$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$

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

Solution:

$a \equiv b \pmod{m} \ \leftrightarrow\ m \mid (a - b)$

(c) What's the Division Theorem?

Solution:

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$, there exist unique integers q, r with $0 \leq r < d$, such that $a = dq + r$.

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) $1 \cdot 2 \cdot 3 \cdot 4|1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

Solution:

(a) True
(b) False
(c) True
(d) True
(e) True

(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) $58 \equiv 707 \pmod{5}$

Solution:

(a) True

(b) True

(c) False

(d) True

(e) False

3. Divisibility Proof

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

Solution:

Let d, n be arbitrary integers, and suppose $d|n$. By definition of divides, there exists some integer k such that $n = dk = 1 \cdot dk$. Note that $-1 \cdot -1 = 1$. Substituting, we see $n = (-1)(-1)dk$. Rearranging, we have $n = (-d)(-1 \cdot k)$. Since k is an integer, $-1 \cdot k$ is an integer because the integers are closed under multiplication. So, by definition of divides, $-d|n$. Since d and n were arbitrary, it follows that for any integers d and n, if $d|n$, then $-d|n$.

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 $a \equiv_n b$.

Solution:

Let integers $n > 1, m > 1$ be arbitrary and integers a, b be arbitrary. Suppose $n \mid m$ and $a \equiv_m b$. By definition of divides, we have $m = kn$ for some integer k. By definition of congruence, we have $m \mid a - b$. By definition of divides, this means that $a - b = mj$ for some integer j. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of divides, we have $n \mid a - b$. By definition of congruence, we have $a \equiv_n b$. Since n, m, a, b were arbitrary, we have shown that if $n \mid m$ and $a \equiv_m b$, 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) $\gcd(9, 6)$

Solution:

$$\begin{aligned}\gcd(9,6) &= \gcd(6,3)\\ &= \gcd(3,0)\\ &= 3\end{aligned}$$

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

Solution:

$$\begin{aligned}\gcd(18,14) &= \gcd(14,4)\\ &= \gcd(4,2)\\ &= \gcd(2,0)\\ &= 2\end{aligned}$$

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

Solution:

$$\begin{aligned}\gcd(80,44) &= \gcd(44,36)\\ &= \gcd(36,8)\\ &= \gcd(8,4)\\ &= \gcd(4,0)\\ &= 4\end{aligned}$$

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

Solution:

$$\begin{aligned}\gcd(77,43) &= \gcd(43,34)\\ &= \gcd(34,9)\\ &= \gcd(9,7)\\ &= \gcd(7,2)\\ &= \gcd(2,1)\\ &= \gcd(1,0)\\ &= 1\end{aligned}$$

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 $a - c \equiv_m b - d$.

Solution:

Let a, b, c, d be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv_m b$ and $c \equiv_m d$. Then by definition of congruence, $m \mid (a-b)$ and $m \mid (c-d)$. Then by definition of divides, there exists some integers k, j such that $a - b = km$ and $c - d = jm$. Then subtracting the second equation from the first, we have:

$$\begin{aligned}(a-b) - (c-d) &= km - jm\\ a - b - c + d &= (k-j)m\\ (a-c) - (b-d) &= (k-j)m\end{aligned}$$

Then by definition of divides, $m \mid (a-c)-(b-d)$. Then by definition of congruence, $a-c \equiv_m b-d$, as desired.

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.

Solution:

We prove by contrapositive. Let $p > 3$ be an arbitrary integer. Suppose that $p \not\equiv 1 \pmod 6$ and $p \not\equiv 5 \pmod 6$. We show that in this case, p is not prime.

Case $p \equiv 0 \pmod 6$**.** Then by definition of congruence, $6 \mid p$. So $p = 6k$ for some integer k. Then p is not prime, since 6 is a factor.

Case $p \equiv 2 \pmod 6$**.** Then by definition of congruence, $6 \mid (p-2)$. Then by definition of divides, $p-2 = 6k$ for some integer k. Then rearranging, we have $p = 6k+2 = 2(3k+1)$. So, p is divisible by 2. Since $p > 3$, it follows that two is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$**.** Then, by definition of congruence, $6|p-3$. Then by definition of divides, $p-3 = 6k$ for some integer k. Rearranging, we have $p = 6k+3 = 3(2k+1)$. So, p is divisible by three. Since $p > 3$, it follows that three is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$**.** Then by definition of congruence, $6 \mid (p-4)$. Then by definition of divides, $p-4 = 6k$ for some integer k. Then rearranging, we have $p = 6k+4 = 2(3k+2)$. So, p is divisible by 2. Since $p > 3$, it follows that two is a factor between 1 and p that is not 1 or p. So, p is not prime.

Since the contrapositive of our statement is true, it follows that the original statement is true as well.