Section 04: Solutions

1. GCD

(a) Calculate gcd(100, 50).

Solution:

$\text{gcd}(50, 100)$ can't be larger than 50 and $50|100$, $\text{gcd}(50, 100) = 50$.

(b) Calculate gcd(17, 31).

Solution:

17 and 31 are two distinct primes. Since each has only 1 and itself as positive divisors, their only common positive divisor is 1, which is therefore their greatest common divisor.

(c) Calculate gcd(9,6)

Solution:

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

(d) Calculate gcd(18,14)

Solution:

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

(e) Calculate gcd(80,44)

Solution:

$$
\begin{aligned}
\gcd(80,40) &= \gcd(44,36) \\
&= \gcd(36,8) \\
&= \gcd(8,4) \\
&= \gcd(4,0) \\
&= 4
\end{aligned}
$$

(f) Calculate gcd(77,43)

Solution:

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

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

Solution:

Let's use guess-and check for some small values We need to find a value for x such that $6x \equiv 1 \pmod 7$.

$$
\begin{aligned}
&6 * 2 = 12, 12\%7 = 5 \\
&6 * 3 = 18, 18\%7 = 4 \\
&6 * 4 = 24, 24\%7 = 3 \\
&6 * 5 = 30, 30\%7 = 2 \\
&6 * 6 = 36, 36\%7 = 1
\end{aligned}
$$

So, for the assignment $x = 6, 6x \equiv 1$ (mod 7).

Thus, the multiplicative inverse of 6 (mod 7) is 6.

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

Solution:

It does not. Intuitively, this is because 49 is a multiple of 7, so 49x for any x is going to be 0 mod 7, which means it can never be 1.

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

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 if $a|b$ and $b|a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution:

Let a, b be arbitrary integers. Suppose $a|b$ and $b|a$. By the definition of divides, we know $a \neq 0$, $b \neq 0$, and $b = ka$ and $a = jb$ for some integers k, j. Combining the equations, we can see that $a = jb = j(ka)$. Dividing both sides by a, we see that $1 = jk$. This means that $\frac{1}{j} = k$. Since both j and k are integers, the only possible solution to this equation is if $j, k \in \{-1, 1\}$. Thus, $a = \pm b$, so $a = b$ 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 $a \equiv b \pmod{n}$.

Solution:

Let integers $n > 1, m > 1$ be arbitrary and integers a, b be arbitrary. Suppose $n|m$ and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some integer k. By definition of congruence, we have $m|a - b$. By definition of divides, this means that $a - b = mj$ for some integer j. Combining the two equations, we see that $a - b = (kn)j = n(kj)$. Since k and j are both integers, kj is also an integer. By definition of divides, we have $n|a - b$. By definition of congruence, we have $a \equiv b \pmod{n}$. Since n, m, a, b were arbitrary, we have shown that if $n|m$ and $a \equiv b \pmod{m}$ 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 $a - c \equiv b - d \pmod{m}$

Solution:

Let a, b, c, d be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by definition of congruence, $m|(a - b)$ and $m|(c - d)$. 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, $m|(a - c) - (b - d)$ and by definition of congruence, $a - c \equiv b - d \pmod{m}$, as desired.

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.

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 p is not prime.

Case $p \equiv 0 \pmod{6}$: By definition of congruence, $6|p$. So $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

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

Case $p \equiv 3 \pmod 6$: 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 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$: By definition of congruence, $6|(p-4)$. 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 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Conclusion: We have shown that in all cases, p is not prime. Since p was arbitrary, for all integers p, if $p > 3$ and $p \not\equiv 1 \pmod 6$ and $p \not\equiv 5 \pmod 6$, then p is not prime.

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

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 $0 \le y < 33$.

Solution:

First, we find the gcd:

$$\begin{aligned} \gcd(33,7) &= \gcd(7,5) & 33 &= \boxed{7} \bullet 4 + 5 & (1)\\ &= \gcd(5,2) & 7 &= \boxed{5} \bullet 1 + 2 & (2)\\ &= \gcd(2,1) & 5 &= \boxed{2} \bullet 2 + 1 & (3)\\ &= \gcd(1,0) & 2 &= 1 \bullet 2 + 0 & (4)\\ &= 1 & & & (5) \end{aligned}$$

Next, we re-arrange equations (1) - (3) by solving for the remainder:

$$\begin{aligned} 1 &= 5 - \boxed{2} \bullet 2 & (6)\\ 2 &= 7 - \boxed{5} \bullet 1 & (7)\\ 5 &= 33 - \boxed{7} \bullet 4 & (8)\\ & & (9) \end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned} 1 &= 5 - \boxed{2} \bullet 2\\ &= 5 - (7 - \boxed{5} \bullet 1) \bullet 2\\ &= 3 \bullet \boxed{5} - 7 \bullet 2\\ &= 3 \bullet (33 - \boxed{7} \bullet 4) - 7 \bullet 2\\ &= 33 \bullet 3 + 7 \bullet -14 \end{aligned}$$

So, $1 = 33 \bullet 3 + \boxed{7} \bullet -14$. Thus, $33 - 14 = 19$ is the multiplicative inverse of 7 mod 33.

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

Solution:

We already computed that 19 is the multiplicative inverse of 7 mod 33. That is, $19 \cdot 7 \equiv 1 \pmod{33}$.

If z is a solution to $7z \equiv 2 \pmod{33}$, then multiplying by 19 on both sides, we have $19 \cdot 7 \cdot z \equiv 19 \cdot 2 \pmod{33}$.

Substituting $19 \cdot 7 \equiv 1 \pmod{33}$ into this on the left gives $1 \cdot z \equiv z \equiv 19 \cdot 2 \equiv 38 \equiv 5 \pmod{33}$.

This shows that every solution z is congruent to 5. In other words, the set of solutions is $\{5 + 33k \mid k \in \mathbb{Z}\}$.