Section 05: Solutions

1. GCD

(a) Calculate gcd(100, 50).

Solution:

50

(b) Calculate gcd(17, 31).

Solution:

1

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

Solution:

6

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

Solution:

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

2. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of $7 \bmod 33$. 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 $0 \leq y < 33$.

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:

$$1 = 5 - \boxed{2} \bullet 2 \quad (6)$$
$$2 = 7 - \boxed{5} \bullet 1 \quad (7)$$
$$5 = 33 - \boxed{7} \bullet 4 \quad (8)$$
$$(9)$$

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

Solution:

If $7y \equiv 1 (\text{mod } 33)$, then

$$2 \cdot 7y \equiv 2 (\text{mod } 33).$$

So, $z \equiv 2 \times 19 (\text{mod } 33) \equiv 5 (\text{mod } 33)$. This means that the set of solutions is $\{5 + 33k \mid k \in \mathbb{Z}\}$.

3. Euclid's Lemma[1]

(a) Show that if an integer p divides the product of two integers a and b, and $\gcd(p, a) = 1$, then p divides b.

Solution:

Suppose that $p \mid ab$ and $\gcd(p, a) = 1$ for integers a, b, and p. By Bezout's theorem, since $\gcd(p, a) = 1$, there exist integers r and s such that

$$rp + sa = 1.$$

Since $p \mid ab$, by the definition of divides there exists an integer k such that $pk = ab$.
By multiplying both sides of $rp + sa = 1$ by b we have,

$$\begin{aligned} rpb + s(ab) &= b \\ rpb + s(pk) &= b \\ p(rb + sk) &= b \end{aligned}$$

Since r, b, s, k are all integers, $(rb + sk)$ is also an integer. By definition we have $p \mid b$.

(b) Show that if a prime p divides ab where a and b are integers, then $p \mid a$ or $p \mid b$. (Hint: Use part (a))

Solution:

[1] these proofs aren't much longer than proofs you've seen so far, but it can be a little easier to get stuck – use these as a chance to practice how to get unstuck if you do!

Suppose that $p \mid ab$ for prime number p and integers a, b. There are two cases.

Case 1: $\gcd(p, a) = 1$
In this case, $p \mid b$ by part (a).

Case 2: $\gcd(p, a) \neq 1$
In this case, p and a share a common positive factor greater than 1. But since p is prime, its only positive factors are 1 and p, meaning $\gcd(p, a) = p$. This says p is a factor of a, that is, $p \mid a$.

In both cases we've shown that $p \mid a$ or $p \mid b$.