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 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 $0 \leq y < 33$.

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:

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

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 $p \mid b$.

4. Have we derived yet?

Each of the following proofs has some mistake in its reasoning - identify that mistake.

(a) *Proof.* If it is sunny, then it is not raining. It is not sunny. Therefore it is raining. □

Solution:

Let p be the proposition that it is sunny and r be the proposition that it is not raining. We know $p \rightarrow \neg r$ and $\neg p$. Using this, the proof shows the inverse $\neg p \rightarrow r$. However, the inverse is not equivalent to the implication, so we cannot infer the inverse from the given statement.

(b) Prove that if $x + y$ is odd, either x or y is odd but not both.

Proof. Suppose without loss of generality that x is odd and y is even.

Then, $\exists k \ x = 2k + 1$ and $\exists m \ y = 2m$. Adding these together, we can see that $x + y = 2k + 1 + 2m = 2k + 2m + 1 = 2(k + m) + 1$. Since k and m are integers, we know that $k + m$ is also an integer. So, we can say that $x + y$ is odd. Hence, we have shown what is required. □

Solution:

Looking at this logically, let's let p be the proposition that $x + y$ is odd and r be the proposition that either x or y is odd but not both. This proof shows $r \rightarrow p$ instead of $p \rightarrow r$.

This proof is incorrect because we have assumed the conclusion. Remember, the converse is not equivalent to the implication.

(c) Prove that $2 = 1$. :)

Proof. Let a, b be two equal, non-zero integers. Then,

$$\begin{aligned}
a &= b \\
a^2 &= ab && \text{[Multiply both sides by a]} \\
a^2 - b^2 &= ab - b^2 && \text{[Subtract } b^2 \text{ from both sides]} \\
(a-b)(a+b) &= b(a-b) && \text{[Factor both sides]} \\
a + b &= b && \text{[Divide both sides by } a - b\text{]} \\
b + b &= b && \text{[Since } a = b\text{]} \\
2b &= b && \text{[Simplify]} \\
2 &= 1 && \text{[Divide both sides by b]}
\end{aligned}$$

□

Solution:

In line 5, we divided by $a - b$. Since $a = b$, $b - a = 0$. Therefore, this was dividing by 0. Dividing by 0 is an undefined operation (!) so this was an invalid step in the proof.

(d) Prove that $\sqrt{3} + \sqrt{7} < \sqrt{20}$

Proof.

$$\sqrt{3} + \sqrt{7} < \sqrt{20}$$
$$(\sqrt{3} + \sqrt{7})^2 < 20$$
$$3 + 2\sqrt{21} + 7 < 20$$
$$19.165 < 20$$

It is true that $19.165 < 20$, hence, we have shown that $\sqrt{3} + \sqrt{7} < \sqrt{20}$ $\square$

Solution:

Like part (b), here too, we have assumed the conclusion was true. In this case, instead of showing that this statement is true, we have shown this statement $\rightarrow T$. Remember, this does not necessarily mean that p is true! If you think back to the truth table for the implication $p \rightarrow q$, the implication becomes a vacuous truth if q is true: we know nothing about the truth value of p.