

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 (mod 7).

Solution:

6

- (d) Does 49 have an multiplicative inverse (mod 7)?

Solution:

It does not. Intuitively, this is because $49x$ for any x is going to be $0 \pmod{7}$, 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:

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

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

$$1 = 5 - \boxed{2} \cdot 2 \tag{6}$$

$$2 = 7 - \boxed{5} \cdot 1 \tag{7}$$

$$5 = 33 - \boxed{7} \cdot 4 \tag{8}$$

$$\tag{9}$$

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

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

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

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

Solution:

If $7y \equiv 1 \pmod{33}$, then

$$2 \cdot 7y \equiv 2 \pmod{33}.$$

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

3. Euclid's Lemma¹

(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,

$$rpb + s(ab) = b$$

$$rpb + s(pk) = b$$

$$p(rb + sk) = b$$

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:

¹these 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. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns true if and only if n is prime (we assume its input is always positive).

```
public boolean isPrime(int n) {
    int potentialDiv = 2;
    while (potentialDiv < n) {
        if (n % potentialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if n is a positive integer.

We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer k being a "nontrivial divisor" of n means that $k \mid n$, $k \neq 1$ and $k \neq n$. Claim: when a positive integer n has a nontrivial divisor, it has a nontrivial divisor at most \sqrt{n} .

- (a) Let's try to break down the claim and understand it through examples. Show an example (a specific n and k) of a nontrivial divisor, of a divisor that is not nontrivial, and of a number with only trivial divisors. **Solution:**

Some examples of "trivial" divisors: (1 of 15), (3 of 3)

Some examples of nontrivial divisors: (3 of 15), (9 of 81)

A number with only trivial divisor is just a prime number: it has no factors.

- (b) Prove the claim. Hint: you may want to divide into two cases!

Solution:

Let k be a nontrivial divisor of n . Since k is a divisor, $n = kc$ for some integer c . Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

We now have two cases:

Case 1: $k \leq \sqrt{n}$

If $k \leq \sqrt{n}$, then we're done because k is the desired nontrivial divisor.

Case 2: $k > \sqrt{n}$

If $k > \sqrt{n}$, then multiplying both sides by c we get $ck > c\sqrt{n}$. But $ck = n$ so $n > c\sqrt{n}$. Finally, dividing both sides by \sqrt{n} gives $\sqrt{n} > c$, so c is the desired nontrivial factor.

In both cases we find a nontrivial divisor at most \sqrt{n} , as required.

Alternate solution (proof by contradiction): Let k be a nontrivial divisor of n . Since k is a divisor, $n = kc$ for some integer c . Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

Suppose, for contradiction, that $k > \sqrt{n}$ and $c > \sqrt{n}$. Then $kc > \sqrt{n}\sqrt{n} = n$. But by assumption we have $kc = n$, so this is a contradiction. It follows that either k or c is at most \sqrt{n} meaning that n has a nontrivial divisor at most \sqrt{n} .

- (c) Informally explain why the fact about integers proved in (b) lets you change the code safely.

Solution:

The new code makes a subset of “checks” that the old code makes, thus the only concern would be that a non-prime number we found in the later checks would “slip through” without the extra checks. However, if a number has any nontrivial divisor, it will have one that is $\leq \sqrt{n}$, so even if we exit the loop early after \sqrt{n} instead of n checks, our method is still guaranteed to always work.

5. Modular Arithmetic

- (a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution:

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers. By the definition of divides, we have $a \neq 0, b \neq 0$ and $b = ka, a = jb$ for some integers k, j . Combining these equations, we see that $a = j(ka)$.

Then, dividing both sides by a , we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$.

- (b) Prove that if $n \mid m$, where 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:

Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod{n}$, as required.

6. Induction with Equality

- (a) Show using induction that $0 + 1 + 2 + \dots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Solution:

For $n \in \mathbb{N}$ let $P(n)$ be “ $0 + 1 + \dots + n = \frac{n(n+1)}{2}$ ”. We show $P(n)$ for all $n \in \mathbb{N}$ by induction on n .

Base Case: We have $0 = \frac{0(0+1)}{2}$ which is $P(0)$ so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show $0 + 1 + \dots + (k + 1) = \frac{(k + 1)(k + 2)}{2}$.

We have

$$\begin{aligned}0 + 1 + \cdots + k + (k + 1) &= (0 + 1 + \cdots + k) + (k + 1) \\ &= \frac{k(k + 1)}{2} + (k + 1) && \text{[Inductive Hypothesis]} \\ &= \frac{k(k + 1)}{2} + \frac{2(k + 1)}{2} \\ &= \frac{k(k + 1) + 2(k + 1)}{2} \\ &= \frac{(k + 1)(k + 2)}{2} && \text{[Factor out } (k + 1)\text{]}\end{aligned}$$

This proves $P(k + 1)$.

Conclusion: $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

- (b) Define the triangle numbers as $\Delta_n = 1 + 2 + \cdots + n$, where $n \in \mathbb{N}$. In part (a) we showed $\Delta_n = \frac{n(n+1)}{2}$. Prove the following equality for all $n \in \mathbb{N}$:

$$0^3 + 1^3 + \cdots + n^3 = \Delta_n^2$$

Solution:

First, note that $\Delta_n = (0 + 1 + 2 + \cdots + n)$. So, we are trying to prove $(0^3 + 1^3 + \cdots + n^3) = (0 + 1 + \cdots + n)^2$. Let $P(n)$ be the statement:

$$0^3 + 1^3 + \cdots + n^3 = (0 + 1 + \cdots + n)^2.$$

We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n .

Base Case. $0^3 = 0^2$, so $P(0)$ holds.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$.

Inductive Step. We show $P(k + 1)$:

$$\begin{aligned}0^3 + 1^3 + \cdots + (k + 1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k + 1)^3 && \text{[Associativity]} \\ &= (0 + 1 + \cdots + k)^2 + (k + 1)^3 && \text{[Inductive Hypothesis]} \\ &= \left(\frac{k(k + 1)}{2}\right)^2 + (k + 1)^3 && \text{[Part (a)]} \\ &= (k + 1)^2 \left(\frac{k^2}{2^2} + (k + 1)\right) && \text{[Factor } (k + 1)^2\text{]} \\ &= (k + 1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]} \\ &= (k + 1)^2 \left(\frac{(k + 2)^2}{4}\right) && \text{[Factor numerator]} \\ &= \left(\frac{(k + 1)(k + 2)}{2}\right)^2 && \text{[Take out the square]} \\ &= (0 + 1 + \cdots + (k + 1))^2 && \text{[Part (a)]}\end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by the principle of induction.