HW6 Individual

CS40 Spring ’22

Bharat Kathi (5938444)

Due: Friday, May 20, 2022 at 11:59PM on Gradescope

Integrity reminders for individual homeworks

- “Individual homeworks” must be solely your own work.
- You may not collaborate on individual homeworks with anyone or seek help from online tutors or entities outside the class.
- You may ask questions about the homework in office hours (of the instructor, TAs, and/or tutors) and on Piazza. However, the staff will only answer clarifying questions on these homeworks. You *cannot* use any online resources about the course content other than the text book and class material from this quarter.
- Do not share written solutions or partial solutions for homework with other students. Doing so would dilute their learning experience and detract from their success in the class.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called “HW6-Individual”.

Proof by Strong Induction To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

Basis Step:	Show the statement holds for b, $b+1$, $\ldots$, $b+j$.
Recursive Step:	Consider an arbitrary integer n greater than or equal to $b+j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b+1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n+1$.

Assigned Questions

1. Group the following numbers according to congruence mod 7:

$$\{25, 8, -4, -142, 113, -3, -30, 10\}$$

Answer: .
Remainder 1: 8 $\equiv$ 113 (mod 7)
Remainder 3: -4 $\equiv$ 10 (mod 7)
Remainder 4: 25 $\equiv$ -3 (mod 7)
Remainder 5: -142 $\equiv$ -30 (mod 7)

2. Group the following numbers according to congruence mod 19:

$$\{22, 15, -35, 34, 72, 79, -111, -42\}$$

Answer: .
Remainder 3: 22 $\equiv$ -35 $\equiv$ 79 $\equiv$ -111 (mod 19)
Remainder 15: 15 $\equiv$ 34 $\equiv$ 72 $\equiv$ -42 (mod 19)

3. Prove by contradiction that $a^2 = b^2 + 1$ has no solutions a, b in the positive integers.

Answer: .
Assume that $a^2 = b^2 + 1$ for some $a \in \mathbb{Z}^+$ and some $b \in \mathbb{Z}^+$.
We can rewrite this as:
$a^2 = b^2 + 1$
$a^2 - b^2 = 1$
$(a + b)(a - b) = 1$
If $b = 0$, then $a = \pm 1$ is a valid solution.
However, since $b \in \mathbb{Z}^+$ then b cannot be equal to 0.
There are now no other integer solutions since b cannot be equal to 0 and $a + b$ and $a - b$ are two distinct integers.
So now the equation $(a + b)(a - b) = 1$ is a factorization of 1 into two distinct integers, which is a contradiction.
Therefore, we can conclude that the assumption that both $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ is false.

4. Give a recursive definition for each of the following sets S. Each set S will be a subset of the set containing all binary strings. A string x belongs to the recursively defined set S if and only if x has each of the following properties (provide a different definition for each part). Note that in each case, you may provide multiple rules for the recursive step of your definition.

   (a) The set S consists of all strings (including the empty string) that have an even number of 1's but may have an even or odd number of zeros.

   Answer: .
   Basis Step: $\lambda \in S$
   Recursive Step:
   If $x \in S$, then $x0 \in S$
   If $x \in S$, then $x11 \in S$
   If $x \in S$, then $1x1 \in S$

(b) The set S consists of all strings (including the empty string) that have the same number of 0's and 1's.

Answer: .

Basis Step: $\lambda \in S$
Recursive Step: .
If $x \in S$, then $0x1 \in S$
If $x \in S$, then $1x1 \in S$
If $x \in S$, then $x01 \in S$
If $x \in S$, then $x10 \in S$

5. Apply your recursive definitions for S for each part of the previous question to construct all elements of S with length less than or equal to 4. Provide your answer in roster notation.

Answer: .

(a) $\{\lambda, 0, 00, 11, 000, 011, 101, 110, 0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$
(b) $\{\lambda, 01, 10, 0011, 0101, 0110, 1001, 1010, 1100\}$

6. RNA is made up of strands of four different bases that match up in specific ways. The bases are elements of the set $B = \{\mathtt{A}, \mathtt{C}, \mathtt{G}, \mathtt{U}\}$.

Definition The set of RNA strands S is defined (recursively) by:

$$\begin{array}{ll} \text{Basis Step:} & \mathtt{A} \in S, \mathtt{C} \in S, \mathtt{U} \in S, \mathtt{G} \in S \\ \text{Recursive Step:} & \text{If } s \in S \text{ and } b \in B, \text{ then } sb \in S \end{array}$$

A function *rnalen* that computes the length of RNA strands in S is defined by:

$$\begin{array}{llll} & & rnalen : S \to \mathbb{Z}^+ & \\ \text{Basis Step:} & \text{If } b \in B \text{ then} & rnalen(b) & = 1 \\ \text{Recursive Step:} & \text{If } s \in S \text{ and } b \in B, \text{ then} & rnalen(sb) & = 1 + rnalen(s) \end{array}$$

Prove by structural induction that $\forall s \in S\ \forall t \in S\ (rnalen(st) = (\ rnalen(s) + rnalen(t)\ )$ by using the recursive definition of *rnalen*.

Answer: .

Proof by structural induction.

Base Case: $t \in B$
$rnalen(st)$ on the left side can be written as $1 + rnalen(s)$ by the inductive step.
$rnalen(s) + rnalen(t)$ on the right side can be written as $rnalen(s) + 1$ by the basis step.
Therefore, $rnalen(st) = rnalen(s) + rnalen(t) = rnalen(s) + 1$

Inductive Step:
Assuming the inductive hypothesis $\forall s \in S(rnalen(st) = rnalen(s) + rnalen(t))$, we will prove that $\forall s \in S(rnalen(stb) = rnalen(s) + rnalen(tb))$, where $b \in B$.
Let $s \in S$ be arbitrary.
$rnalen(stb) = 1 + rnalen(st)$, by the recursive step
$= 1 + rnalen(s) + rnalen(t)$, by the inductive hypothesis

$= rnalen(s) + rnalen(tb)$, by the recursive step $(rnalen(tb) = 1 + rnalen(t))$

Therefore, our inductive hypothesis is proven true.

7. Some numbers and their prime factorizations are given below.

   - $140 = 2^2 \cdot 5 \cdot 7$
   - $175 = 5^2 \cdot 7$
   - $1083 = 3 \cdot 19^2$
   - $25480 = 2^3 \cdot 5 \cdot 7^2 \cdot 13$

   Use these prime factorizations to compute the following quantities and justify your answers.

   (a) $gcd(1083, 175)$

   Answer: 1

   (b) $gcd(25480, 140)$

   Answer: $2^2 * 5 * 7 = 140$

   (c) $gcd(175, 140)$

   Answer: $5 * 7 = 35$

8. Prove the gcd lemma: For any positive integers x, y, not both zero, $y \geq x$, $gcd(y, x) = gcd(y - x, x)$

   Answer: .

   Let z = y - x.
   We will prove that some number n is a factor of y and x only if it is a factor of both x and z.
   This implies that the set of common divisors of y and x are the same as the set for x and z.
   Then the gcd(x,y) must be the largest number in this set, making it also the gcd(x,z).

   Let's prove that if $n|y$ and $n|x$, then $n|z$ and $n|x$.
   Assuming that $n|y$ and $n|x$, we can say that $y = an$ for some integer n, and that $x = bn$ for some interger b.
   Plugging these equations into $z = y - x$ gives us $z = an + bn = (a + b)n$.
   Since we know that a and b are integers, a+b must also be an integer.
   Since a+b is an integer and n is nonzero, we know that $n|z$.

   Now we prove that if $n|z$ and $n|x$, then $n|y$ and $n|x$.
   Assuming that $n|z$ and $n|x$, we can say that $z = cn$ for some integer c, and that $x = dn$ for some integer d.
   We can plug these into $z = y - x$ and simplify to get that $y = cn + dn(c + d)n$.
   Since we know that c and d are integers, c+d must also be an integer.
   Since c+d is an integer and n is nonzero, we know that $n|y$.

   Therefore, we know that some number n is a factor of y and x only if it is a factor of both x and z.

9. Use the gcd lemma from the previous question and strong induction to prove the gcd theorem:

   For any positive integers x, y, not both zero, $y \geq x$, $gcd(y, x) = gcd(x, y \textbf{ mod } x)$.

Note: We proved the theorem in lecture using a different method. For the homework we will only accept solutions that use induction.

Answer: .

Proof by strong induction.
Base Case: $y = x$
On the left hand side, $gcd(x, x) = x$
On the right hand side, $gcd(x, x \ mod \ x) = gcd(x, 0) = x$

Inductive Step: For $y \geq x$, assume as the inductive hypothesis that $gcd(i, x) = gcd(x, i \ mod \ x)$ for every i where $x \leq i \leq y$.
We will prove that $gcd(y + 1, x) = gcd(x, (y + 1) \ mod \ x)$.
From our above lemma, we know that we have two cases now.

Case 1: $y + 1 - x < x$
Since $0 \leq y + 1 - x < x$, then $r = y + 1 - x$ where $n = qd + r$ (the division algorithm).
So $y + 1 - x = (y + 1) \ mod \ x$.
Therefore, $gcd(y + 1, x) = gcd(x, (y + 1) \ mod \ x)$.

Case 2: $y + 1 - x \geq x$
Since $x \leq y + 1 - x \leq y$, then $y + 1 - x$ must fall in the range mentioned in our inductive hypothesis.
Thsi means that $gcd(y + 1 - x, x) = gcd(x, (y + 1 - x) \ mod \ x)$.
We know that $y + 1 - x = y + 1 \ (mod \ x)$, so $gcd(y + 1, x) = gcd(x, (y + 1) \ mod \ x)$.

10. For positive integers a, b, and c prove that if $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Answer: .

Let a,b,c be arbitrary positive integers.
Assume that $gcd(a, b) = 1$ and that $a|bc$.
We will use this to prove that $a|c$.

Using Euclid's algorithm, we know that $gcd(a, b)$ can be written as a linear combination of a and b.
$gcd(a, b) = 1$
$sa + tb = 1$
$sac + tbc = c$, multiplying both sides by c.
We can see now that $a|sac$ and $bc|tbc$, and since we are asssuming $a|bc$, we can also know that $a|tbc$.
Since $a|sac$ and $a|tbc$, we have proves that a also divides $sac + tbc$, which is equal to c.

11. Write proofs and algorithms related to finding base 2 expansions

(a) Use strong induction to prove the theorem: Every positive integer is a sum of (one or more) distinct powers of 2. *You are essentially proving that binary expansions exist!*

(b) In lecture you were presented with two algorithms for finding the base 2 expansion of any positive integer. Complete the outline of the algorithm below to recursively compute the base 2 expansion of a positive integer.

Algorithm: Calculating base 2 expansion recursively

```
procedure base2recursive(n: a positive integer)

if (n = 0) $a_0$ := 0
if (n = 1) $a_0$ := 1
if (n > 2) {
    ($a_{k-1}$ ,... ,$a_1$) := base2recursive(n div 2)
}

return $(a_{k-1}, \ldots, a_0)\{(a_{k-1} \ldots a_0)_b$ is the base 2 expansion of $n\}$
```

12. Prove that $n \in \mathbb{N}$ is divisible by 3 if and only if the alternating sum of the bits of n in binary representation is divisible by 3. The alternating sum of any sequence $a_0, a_1, ..., a_m$ is $\sum_{i=0}^{m} (-1)^i a_i$

Attributions

Thanks to Mia Minnes and Joe Politz for the original version of Q6. All materials created by them is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.