CS135 Sample Test 2

Closed book: no textbook, no electronic devices; two sheets of paper with notes, to hand in with the test. There are a total of 105 points but the max credit allowed is 100.

NOTE: this is a previous test that covered some topics in number theory that we haven't covered yet in 2015.

Question 1 *(20 points)* Consider this function.

```
(define (numInRange lo hi lon)
  ; How many elements of lon are in range lo..hi, inclusive.
  ; Assuming lon is a list of numbers, and lo and hi are numbers
  (cond [(null? lon) 0]
        [(and (>= (car lon) lo) (<= (car lon) hi))
         (+ 1 (numInRange lo hi (cdr lon)))]
        [else (numInRange lo hi (cdr lon))]))
```

For example, `(numInRange 1 5 '(2 3 0 6 4))` returns 3.

Your task: complete the following code so that `numInRangeTrec` does the same thing, but using a tail-recursive helper.

```
(define (numInRangeTrec lo hi lon)
  (nIRhelp lo hi lon 0))

(define (nIRhelp lo hi lon n)
    ...TO DO...
```

SOLUTION

```
(define (nIRhelp lo hi lon n)
  (cond [(null? lon) n]
        [(and (>= (car lon) lo) (<= (car lon) hi))
         (nIRhelp lo hi (cdr lon) (+ 1 n))]
        [else (nIRhelp lo hi (cdr lon) n)]))
```

Question 2 *(5 points)* Show a trace of `(numInRangeTrec 1 5 '(2 3 0 6))` using your definition of `nIRhelp`. Just show the calls to these two functions.

SOLUTION

```
(numInRangeTrec 1 5 '(2 3 0 6))
  (nIRhelp 1 5 '(2 3 0 6) 0)
    (nIRhelp 1 5 '(3 0 6) 1)
      (nIRhelp 1 5 '(0 6) 2)
        (nIRhelp 1 5 '(6) 2)
          (nIRhelp 1 5 '() 2)
          returns 2
```

Question 3 *(10 points)* This question is about the following functions.

```
(define (length xs)
  (cond [(null? xs) 0]
        [else (+ 1 (length (cdr xs)))]))
(define (stutter xs)
  (cond [(null? xs) '()]
        [else (cons (car xs)
                    (cons (car xs)
                          (stutter (cdr xs))))] ))
```

Theorem: `(length (stutter xs)) = (* 2 (length xs))` for all lists `xs`

This can be proved by induction. For this question: prove the base case. Justify every step.

Base case: `(length (stutter '()))` = `(* 2 (length '()))`
SOLUTION: (By the way, this was in Homework 6.)
Proof of base case: by definitions. That's the succinct way of saying it, since the details are easy to work out. But your job is to show you understand the details. Here's what I'm looking for:
Proof of base case:

```
  (length (stutter '()))
= (length '())             by def stutter
= 0                        by def length
= (* 2 0)                  by arith
= (* 2 (length '()))       by def length
```

That layout was easy for me because I had plenty of time to make it readable. But you could also do the calculation like this:

```
    (length (stutter '()))
  = (length '())             by def stutter
  = 0                        by def length

and
    (* 2 (length '()))
  = (* 2 0)                  by def length
  = 0                        by arith

so left side equals right side.
```

Or draw a line connecting the zeros.

IMPORTANT: have a look at this quasi-nonsense:

```
(length (stutter '())) = (* 2 (length '()))
          (length '()) = (* 2 (length '()))  by def stutter
                     0 = (* 2 0)             by def length
                     0 = 0                   by arith
```

What's the connection between the lines??!! Usually reasoning goes forward, but here what's important is backward: we're trying to prove that the first line is true. So we reduce it to $0 = 0$. (And $0 = 0$ is true, because equality is reflexive, as any educated reader should know.) We should make that clear by writing the logical connection between the lines, which happens to be equivalence.

I decided not to take points off for not making the connection clear, even though I have ranted and raved about this several times in class. It appears that many of you have been brainwashed by previous study and are having difficulty getting over it:)

If you think I'm being silly, have a look at this "proof" that 50 is 100.

```
      50 = 100
      25 = 50         by arithmetic (divide by 2)
25 mod 5 = 50 mod 5   by arithmetic (take remainder)
       0 = 0          by arithmetic (calculate remainder)
```

What went wrong? Doesn't each line follow from the previous one?

Question 4 *(15 points)* Continuing from the previous question, here is the inductive case. Provide the missing justifications (marked "???").

Inductive case, for any non-null `xs`: `(length (stutter xs))` = `(* 2 (length xs))`

Inductive hypothesis: `(length (stutter (cdr xs)))` = `(* 2 (length (cdr xs)))`

Proof of inductive case:

```
    (length (stutter xs))

  = (length (cons (car xs) (cons (car xs) (stutter (cdr xs))))) by def stutter

  = (+ 1 (length (cons (car xs) (stutter (cdr xs))))) by ???

  = (+ 1 (+ 1 (length (stutter (cdr xs)))))           by ???

  = (+ 2 (length (stutter (cdr xs))))                 by arithmetic

  = (+ 2 (* 2 (length (cdr xs))))                     by ???

  = (* 2 (+ 1 (length (cdr xs))))                     by arithmetic

  = (* 2 (length xs))                                 by def length
```

SOLUTION: by definition of `length`; by definition of `length`; by inductive hypothesis.

Question 5 *(3 points)* Which of these numbers are congruent to 3, modulo 7?

(a) 37

(b) 66

(c) -17

SOLUTION Only (b). Because $66 \equiv 3 (\bmod 7)$ means, by definition, $7 \mid (66 - 3)$, and 7 does divide 63. (You could as well interpret "congruent to 3" to mean $3 \equiv 66 (\bmod 7)$, in which case the condition is $7 \mid -63$, also true.) Several people thought about this in terms of division: $66 = 3 + 9 \cdot 7$.

Not (a) since 7 doesn't divide $37 - 3$. Or you could notice $37 = 2 + 5 \cdot 7$.

Not (c) since $-17 = 4 + 7 \cdot -3$.

Question 6 *(8 points)* Which properties does the "divides" relation have?

reflexive?

symmetric?

antisymmetric?

transitive?

SOLUTION Reflexive, antisymmetric, transitive. Not symmetric.

Question 7 *(5 points)* For any $m > 0$, the relation "congruent modulo m" is symmetric. Write a formula to express this property.
SOLUTION Here is one.

$$\forall a, b. \quad a \equiv b(\text{mod}\, m) \to b \equiv a(\text{mod}\, m)$$

Anything logically equivalent to this is also acceptable. For example, it happens that we get the same property using $\leftrightarrow$ instead of $\to$. (But be careful, in most situations $\leftrightarrow$ isn't interchangeable with $\to$.)

IMPORTANT: $a \equiv b(\text{mod}\, m)$ is equivalent to $m \mid a - b$ (by definition) and it's also equivalent to $a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$ (a theorem). It is *not* equivalent to $a \,\mathbf{mod}\, m = b$.

Here is a long-winded way of saying congruence is symmetric:

$$\forall a, b. \quad R(a, b) \to R(b, a) \text{ where } R(x, y) \text{ means } x \equiv y(\text{mod}\, m)$$

In other words, R is symmetric, where R is congruence modulo m.

My phrase "this property" wasn't meant to include the "for any m", but the sentence is ambiguous. So I gave full credit for this reasonable interpretation:

$$\forall m > 0. \, (\forall a, b. \quad a \equiv b(\text{mod}\, m) \to b \equiv a(\text{mod}\, m) \;)$$

By the way, the domain of a and b should be all integers, not just positive ones, but I'm not requiring the domain to be specified here.

Question 8 *(5 points)* For any $m > 0$, the relation "congruent modulo m" is transitive. Write a formula to express this property.
SOLUTION

$$\forall a, b, c. \quad a \equiv b(\text{mod}\, m) \land b \equiv c(\text{mod}\, m) \to a \equiv c(\text{mod}\, m)$$

By the way, the symbol for "and" is $\land$. Or use &. The carat symbol ^ is just what you use if your text editor doesn't have the right symbol (although `/\` looks ok in many fonts).

Question 9 *(4 points)* Fill in the greatest common divisors. Justify your answer by showing the divisors.

a	b	gcd(a,b)
7	5	
7	10	
21	20	
21	30	

SOLUTION

a	b	gcd(a,b)
7	5	1
7	10	1
21	20	1
21	30	3

Divisors of 10 are 1,2,5,10. Divisors of 21 are 1,3,7,21. Divisors of 20 are 1,2,5,10,20. Divisors of 30 are 1,2,3,5,6,10,15,30.

Question 10 *(5 points)* Define "a is relatively prime to b".
SOLUTION $gcd(a, b) = 1$, or in words "the greatest common divisor of a and b is 1." Of course there are other equivalent conditions, like $\neg(\exists n > 1.\ n \mid a \wedge n \mid b)$.

Question 11 *(5 points)* Which integers less than 12 are relatively prime to 12? **SOLUTION** 5, 7, 11

Note: According to the definition, 1, -1, -5, -7, -11 also qualify, in fact even -13, -25, and others. So I'll accept those as answers but not require them since usually this concept is used with positive integers.

Question 12 *(5 points)* Find an inverse of 5 modulo 7. That is, find x such that $x \cdot 5 \equiv 1 (\mathrm{mod}\ 7)$.
SOLUTION

One inverse is 3, because $3 \cdot 5 = 15$ and $15\ \mathbf{mod}\ 7 = 1$. Anything else congruent to 3, modulo 7, is also an inverse, e.g., 10, 17, 24,. . . , and also -4, -11, -18,. . .

Question 13 *(15 points)* Below is a proof with missing justifications marked by "???". Fill those in, referring to the facts listed at the end of the test.

Theorem: If $a \equiv b(\mathrm{mod}\ m)$ and $c \equiv d(\mathrm{mod}\ m)$ then $a + c \equiv b + d(\mathrm{mod}\ m)$.

Proof:
1. $a \equiv b(\mathrm{mod}\ m)$ and $c \equiv d(\mathrm{mod}\ m)$ by assumption
2. $a = km + b$ and $c = k'm + d$ for some k, k' from 1 by ??? **SOLUTION**: fact (b)
3. $a + c = (k + k')m + (b + d)$ from 2 by ??? **SOLUTION**: arithmetic
4. $a + c \equiv b + d(\mathrm{mod}\ m)$ from 3 by ??? **SOLUTION**: fact (b)

SOLUTION: See above. Note that for step 4, I instantiated (b) with $a+c$ in place of a, $k + k'$ in place of c, and $b + d$ in place of b.

Several people said that steps 2 and 4 are by definition of "congruence modulo". But it's clear in both Rosen and my slides that we chose to use the $m \mid a - b$ definition (see below). Yes, there are equivalent conditions, like (a) and (b) (which is also known as Theorem 4).

It's true that one could have chosen one of those as the definition, and then proved the other conditions are equivalent.

Some definitions:

Divides: $b \mid c$ iff $\exists d\ (c = b * d)$
Congruence: $a \equiv b(\mathrm{mod}\ m)$ iff $m \mid a - b$

Facts: (for all integers a, b, c, d, n and all $m \in \mathbf{Z}^+$)

(a) $a \equiv b(\mathrm{mod}\ m)$ iff $a\ \mathbf{mod}\ m = b\ \mathbf{mod}\ m$
(b) $a \equiv b(\mathrm{mod}\ m)$ iff $\exists c.\ a = cm + b$
(c) If $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$
(d) $a = (a\ \mathbf{div}\ m) \cdot m + (a\ \mathbf{mod}\ m)$
(e) If $a \equiv b(\mathrm{mod}\ m)$ and $c \equiv d(\mathrm{mod}\ m)$
then $a + c \equiv b + d(\mathrm{mod}\ m)$ and $ac \equiv bd(\mathrm{mod}\ m)$
(f) $(a + b)\ \mathbf{mod}\ m = ((a\ \mathbf{mod}\ m) + (b\ \mathbf{mod}\ m))\ \mathbf{mod}\ m$
(g) $ab\ \mathbf{mod}\ m = ((a\ \mathbf{mod}\ m)(b\ \mathbf{mod}\ m))\ \mathbf{mod}\ m$

Linear combination Thm: $\forall a, b \in \mathbf{Z}^+.\ \exists s, t \in \mathbf{Z}.\ gcd(a, b) = sa + tb$
Divisibility Lemma: if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.
Cancellation Thm: If $ac \equiv bc (\bmod m)$ and $gcd(c, m) = 1$ then $a \equiv b (\bmod m)$.
Inverse Thm: $gcd(a, m) = 1$ iff $\exists \overline{a}.\ \overline{a}a \equiv 1 (\bmod m)$ (for all $m > 1$)