WORKSHEET #6 – MATH 2200
SPRING 2018

NOT WEDNESDAY

This should help you prepare for the midterm.

1. Short answer questions.

(a) Define what it means for a function $f : A \longrightarrow B$ to be injective.

Solution: For every $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$.

(b) Is it true that there is a solution to $3x \equiv_9 1$?

Solution: No.

(c) What is the definition of the $\gcd(a, b)$?

Solution: It is the greatest integer that is a factor of both a and b.

(d) State Fermat's little theorem.

Solution: There is more than one way to phrase this. Here's one I'd take. If p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv_p 1$.

(e) Suppose that $[a]$ and $[b]$ are two distinct equivalence classes of an equivalence relation $\sim$. Is it possible that $a \sim b$?

Solution: No, since $[a]$ and $[b]$ are distinct, they have some terms not in common. Thus $[a] \neq [b]$. But equivalence classes are either equal or disjoint, ie in our case $[a] \cap [b] = \emptyset$. Thus a is not equivalent to b.

(f) Consider the function $f(x) = 3x^3 + 2^x$. True or false, $f(x)$ is $O(x^3)$?

Solution: No, the 2^x term makes that impossible.

(g) Consider the system of congruences $x \equiv_{11} 7$ and $x \equiv_{13} 3$. How many solutions does this system have between 0 and $142 = 11 \cdot 13 - 1$?

Solution: Only 1 solution (by the Chinese remainder theorem).

(h) What's the smallest prime integer bigger than 100?

Solution: 1009. (This is probably too computational for an actual exam).

(i) Define what it means that a relation is an equivalence relation.

Solution: It must be reflexive, symmetric and transitive.

(j) Do an insertion sort, showing all the steps, on the integers $\{3, 0, 5, -1\}$.

Solution:

Step 1: $\{3, 0, 5, -1\}$ (we've sorted the first item)
Step 2: $\{0, 3, 5, -1\}$ (we've sorted the first two items)
Step 3: $\{0, 3, 5, -1\}$ (we've sorted the first three items)
Step 4: $\{-1, 0, 3, 5, \}$ (we've sorted the first four items)

(k) Write the number 23 in base 6.

Solution: $(35)_6$

(l) Rewrite the base 5 integer $(401)_5$ as an integer in base 10.

Solution: 401 is $(4 \cdot 5^2) + (0 \cdot 5^1) + (1 \cdot 5^0) = 101$.

(m) At most how many comparisons does a binary search do on a list of length n (you may use big O notation).

Solution: $O(\log n)$

(n) If φ is the Euler phi function, what is $\varphi(45)$?

Solution: $45 = 3^2 \cdot 5$ so $\varphi(45) = (3^2 - 3)(5 - 1) = 24$.

2. Run the extended Euclidean algorithm on the integers 121 and 77 and use it to find integers s and t such that $s \cdot 121 + t \cdot 77 = 11$. Make sure to explain each step.

Solution: First we divide $121 = a_1$ by $77 = b_1$, we get $121 = q_1 77 + r_1$ where $q_1 = 1$ and $r_1 = 44$.
Next we divide $77 = a_2$ by $44 = b_2$, we get $77 = q_2 44 + r_2$ where $q_2 = 1$ and $r_2 = 33$.
Next we divide $44 = a_3$ by $33 = b_3$, we get $44 = q_3 33 + r_3$ where $q_3 = 1$ and $r_3 = 11$.
Finally we divide $33 = a_3$ by $11 = b_4$, we get $33 = q_4 11 + r_4$ where $q_4 = 3$ and $r_4 = 0$.
Now we work backwards. At this point we have written $11 = 44 + (-1)33 = a_3 + (-1)b_3$. But $b_2 = a_3$ and $a_2 = b_2 + b_3$ and so

$$11 = b_2 + (-1)(a_2 - b_2) = 2b_2 + (-1)a_2.$$

Next we see that $b_1 = a_2$ and $a_1 = b_1 + b_2$ and so

$$11 = 2(a_1 - b_1) + (-1)b_1 = 2a_1 + (-3)b_1$$

and so $s = 2$ and $t = -3$.

3. Solve the system of congruences

$$\begin{aligned} 2x &\equiv_5 3 \\ x &\equiv_3 5 \\ 3x &\equiv_4 0 \end{aligned}$$

Solution: The first becomes $x \equiv_5 9 \equiv_5 4$ by multiplying by 3. The second simplifies to $x \equiv_3 2$. The last becomes $x \equiv_4 0$ by multiplying by 3.

Now we find the solution. I'll do this in a fast ad-hoc way, that you might be able to emulate on future exams (see the quiz for a example using the book's strategy). I first notice that $x = 4$ is definitely a solution to the first and third congruence, and so a solution to $x \equiv_{20} 4$ (which is just a way to rewrite the first two congruences in a single congruence).

Now I have to solve $x \equiv_{20} 4$ and $x \equiv_3 2$ simultaneously. The solutions to the first are $\{\dots, 4, 24, 44, 64, \dots\}$. We see immediately that 44 is a solution to the second. Hence we have solved the system with $x = 44$. Note the other solutions are just the solutions to

$$x \equiv_{60} 44$$

or in other words $x = 44 + 60k$ where $k \in \mathbb{Z}$.

4. Describe an algorithm that determines if a function $f : \{1, 2, 3, 4, 5\} \longrightarrow \{6, 7, 8, 9\}$ is surjective. You may use pseudo-code or sentences.

Solution: I'll give a pseudocode algorithm.

```
isSurjective(f)
    let L = (6, 7, 8, 9) %a list of desired outputs
    for i = 1 to 5 do
        let val = f(i)
        for j = 1 to |L| do
            if (L[j] == val) then
                L = RemoveEntry(j, L) %removes the jth entry from L
                break %exit the inner loop
            end if
        loop
    loop
    if |L| = 0 then
        return true
    else
        return false
```

The idea is we have a list of outputs we want. As we find outputs the function outputs, we remove them from the list. If our list of outputs is empty, the function must have been surjective.

5. Describe an algorithm that computes $\varphi(n)$ where the input n is an integer. How many times does it run the Euclidean Algorithm? (You may assume you already have a different function that has implemented the Euclidean Algorithm).

Solution: I'll describe this algorithm in words.

Make a counter variable `counter = 0`. Start a loop that takes `i` from 1 to $n - 1$. If at any step in the loop `gcd(i, n) = 1` then increase the counter

```
counter = counter + 1
```

Note I'm imagining we already have a `gcd` function (as said). After the loop completes simply `return counter`.

Note this function runs `gcd` $n - 1$ times. Thus it is exponential if viewed in terms of the number of digits of n.

6. Fix an integer $n > 0$. Write $a \equiv_n b$ (for integers a and b) if $n|(a-b)$. Prove carefully that $\equiv_n$ is an equivalence relation.

Solution: We must show the relation is reflexive, symmetric and transitive.

Reflexive: We must show that $a \sim a$ or in other words that $n|(a-a)$, but that's just saying that $n|0$, and everything divides 0, so our relation is reflexive.

Symmetric: Suppose $a \sim b$, or in other words that $n|(a-b)$. We must show that $n|(b-a)$. But $(b-a) = -(a-b)$ and so the relation is symmetric, as desired.

Transitive: Suppose $a \sim b$ and $b \sim c$. We know that $n|(a-b)$ so that $(a-b) = nk$, and also that $n|(b-c)$ so that $b-c = nk'$. Adding these two equations we get that

$$a - b + b - c = nk + nk'$$

Thus

$$a - c = n(k + k')$$

and so $n|(a-c)$ and therefore $a \sim c$ as we wanted.

7. Consider the set $S = \mathbb{Z} \times \mathbb{Z}$ (the set of ordered pairs of two integers). We define an relation $\sim$ on S by declaring $(a,b) \sim (c,d)$ if $a^2 + b^2 = c^2 + d^2$.

(a) Prove that $\sim$ is an equivalence relation.

Solution: We must show the relation is reflexive, symmetric and transitive.

Reflexive: We must show that $(a,b) \sim (a,b)$, but it suffices to show that $a^2 + b^2 = a^2 + b^2$ which is tautological and so the relation is indeed reflexive.

Symmetric: We must show that if $(a,b) \sim (c,d)$ then $(c,d) \sim (a,b)$. So suppose $(a,b) \sim (c,d)$, then $a^2 + b^2 = c^2 + d^2$. Hence $c^2 + d^2 = a^2 + b^2$ which implies that $(c,d) \sim (a,b)$ as desired.

Transitive: Finally suppose that $(a,b) \sim (c,d)$, and $(c,d) \sim (e,f)$. Then $a^2 + b^2 = c^2 + d^2$ and $c^2 + d^2 = e^2 + f^2$. Thus $a^2 + b^2 = e^2 + f^2$ so $(a,b) \sim (e,f)$ and the relation is indeed transitive.

(b) Compute $\left|[(1,0)]_\sim\right|$ (the size of the equivalence class of $(1,0)$).

Solution: We observe that $[(1,0)]_\sim$ is the set of $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ so that $a^2 + b^2 = 1^2 + 0^2 = 1$. There are only four pairs of integers that satisfy that, $(\pm 1, 0)$ and $(0, \pm 1)$. Thus the size of the equivalence class is 4.