CS 70, Summer 2014 — Homework 2

Harsimran (Sammy) Sidhu, SID 23796591

July 7, 2014

Collaboraters: Chonyi Lama, Jenny Pushkarskaya
Sources: http://comet.lehman.cuny.edu/sormani/teaching/induction.html

Problem 1

(a) $\forall n > 0$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^n \leq \begin{bmatrix} 2n & 2n \\ 2n & 2n \end{bmatrix}$$

Proof: Define $A(x)$ to be

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^n$$

Base Cases:
let $n = 1$

$$A(1) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \leq \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$$ Valid

let $n = 2$

$$A(2) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = A(1) \times \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \leq \begin{bmatrix} 4 & 4 \\ 4 & 4 \end{bmatrix}$$ Valid

let $n = 3$

$$A(3) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^3 = A(2) \times \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix} \leq \begin{bmatrix} 6 & 6 \\ 6 & 6 \end{bmatrix}$$ Valid

Strengthing the Hypothesis: From the base cases it seems that

$$A(n) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}$$

Which is obviously ($\leq 2n$) for every entry.

Inductive Hypothesis: $A(k) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 2k \\ 0 & 1 \end{bmatrix}$

let $n = k + 1$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & 2(k+1) \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^k \times \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2k+2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2k \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2k+2 \\ 0 & 1 \end{bmatrix}$$ Substitute Inductive Hypothesis

$$\begin{bmatrix} (1 \times 1 + 0 \times 2k) & (1 \times 2 + 2k \times 1) \\ (0 \times 1 + 1 \times 0) & (0 \times 2 + 1 \times 1) \end{bmatrix} = \begin{bmatrix} 1 & 2k+2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2k+2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2k+2 \\ 0 & 1 \end{bmatrix}$$ Valid

(b) $\forall c \geq 12\ \exists (m, n) \in \mathbb{N}\ (3m + 7n = c)$ Original Statement

m is the number of 3 cent coins and n is the number of 7 cent coins

Base Cases:

$(c = 12) \rightarrow (m = 4, n = 0) \rightarrow (3(4) + 7(0) = 12)$

$(c = 13) \rightarrow (m = 2, n = 1) \rightarrow (3(2) + 7(1) = 13)$ (m=m-2, n=n+1)

$(c = 14) \rightarrow (m = 0, n = 2) \rightarrow (3(0) + 7(2) = 14)$ (m=m-2, n=n+1)

Inductive Hypothesis: Suppose we can make form any integer value of cents from 12 to k. We need to show that we can make $k + 1$ cents using only 3-cent and 7-cent coins

Since we proved base cases to 14, we'll assume $k + 1 \geq 15$

$k + 1 \geq 15$

$(k + 1) - 3 \geq 15 - 3$

$(k + 1) - 3 \geq 12$

$(k + 1) - 3 = 3m + 7n$

$(k + 1) = 3(m + 1) + 7n$ valid

(c) $\forall n \in \mathbb{N}\ (F_n = \frac{\phi^n-(1-\phi)^n}{\sqrt{5}})$ where $\phi = \frac{1+\sqrt{5}}{2}$
$(F_n = F_{n-2} + F_{n-1})$ where $F_0 = 0,\ F_1 = 1$

Proof: $F_n = \frac{\phi^n-(1-\phi)^n}{\sqrt{5}} = F_{n-2} + F_{n-1}$

Base Cases:
$n = 0 \rightarrow \frac{\phi^0-(1-\phi)^0}{\sqrt{5}} = 0$ True
$n = 1 \rightarrow \frac{\phi^1-(1-\phi)^1}{\sqrt{5}} = \frac{\phi-1+\phi}{\sqrt{5}} = \frac{2\phi-1}{\sqrt{5}} = \frac{1+\sqrt{5}-1}{\sqrt{5}} = 1$ True
Inductive Hypothesis: Assume $F_k = \frac{\phi^k-(1-\phi)^k}{\sqrt{5}}$ is true for integers $0 \leq k$
We now need to show $F(k)$ for $k \geq 2$
let $n = k + 2$ Will hit either of the two base cases

$F_{k+2} = \frac{\phi^{k+2}-(1-\phi)^{k+2}}{\sqrt{5}} = \frac{\phi^2\phi^k-(1-\phi)^2(1-\phi)^k}{\sqrt{5}}$ Factor out
$\phi^2 = (\frac{1+\sqrt{5}}{2})^2 = \frac{6}{4} + \frac{\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \phi$
$(1-\phi)^2 = (1 - \frac{1+\sqrt{5}}{2})^2 = (\frac{1-\sqrt{5}}{2})^2 = \frac{6}{4} - \frac{\sqrt{5}}{2} = 1 + \frac{1-\sqrt{5}}{2} = (1 + (1-\phi))$

$F_{k+2} = \frac{\phi^k(1+\phi)-(1-\phi)^k(1+(1-\phi))}{\sqrt{5}} = \frac{\phi^k+\phi^{k+1}-(1-\phi)^k-(1-\phi)^{k+1}}{\sqrt{5}}$ Simplify
$F_{k+2} = \frac{\phi^k-(1-\phi)^k}{\sqrt{5}} + \frac{\phi^{k+1}-(1-\phi)^{k+1}}{\sqrt{5}}$ Group by order
$F_{k+2} = F_k + F_{k+1}$ Substitute hypothesis
$F_k = F_{k-2} + F_{k-1}$ Valid

(d) $\forall n \geq 2 \in \mathbb{N}\ f(n) = 7f(n-1) - 10f(n-2)$ where $f(0) = 1,\ f(1) = 2$
table $f(n)$
$f(0) = 1$ True
$f(1) = 2$ True
$f(2) = 4$
$f(3) = 8$
$f(4) = 16$

Proof: $f(n) = 7f(n-1) - 10f(n-2) = 2^n$ with Induction on n Fits the table
Inductive hypothesis: Assume $f(k) = 2^k$ for all n between 2 and k. We now need to show that $f(k+1) = 2^{k+1}$

let $n = k + 1$
$f(k+1) = 7f(k) - 10f(k-1) = 7 \times 2^k - 10 \times 2^{k-1}$ Substitute hypothesis
$f(k+1) = 7f(k) - 10f(k-1) = 7 \times 2^k - 10 \times 2^{k-1}$
$f(k+1) = 7f(k) - 10f(k-1) = 7 \times 2^k - 5 \times 2^k$
$f(k+1) = 7f(k) - 10f(k-1) = 2 \times 2^k$
$f(k+1) = 7f(k) - 10f(k-1) = 2^{k+1}$
$f(k+1) = 2^{k+1}$ Valid

Problem 2

(a) True, if man M and woman W put each other on top of their respective preference list and they are both paired with other people then they will always be a rogue couple.

(b) False, if man M and woman W are on the bottom of everyone's preference list then they would be paired to one another with no rogue couples existing.

(c) True, there exists a stable marriage instance where every unmatched couple is a rogue couple. If all the men were matched to their unique least preferred woman and the the women also preferred that man the least uniquely then every couple would be a rogue couple.

Problem 3

(a) **Every Morning:** Each student goes to the hospital on top of their list that they haven't crossed off yet

Every Afternoon: Each hospital h says to come back the next day to the top q_h students (from prior day's waitlist and new proposals) and adds them to their waitlist. Then each hospital h rejects their respective non-top students that were proposals or prior waitlisters that are no longer in the top q_h and have been bumped out.

Every Night: Each rejected student then crosses off the hospital h that rejected them.

The loop is repeated until all students that are unpaired have been rejected from all hospitals and all the slots for have been filled for each hospital h. Each hospital h now accepts the q_h students on their waitlist.

(b) **Improvement Lemma:** For each hospital h, after its waitlist becomes full, its least favorite student on the waitlist can only improve over time.

Suppose a proof by contradiction, that hospital h's least favorite student becomes worse with each day. On day k hospital h has a student s that is its least favorite. On day $k+1$, student $s\prime$ proposes to hospital h. Since our algorithm states that hospital h bumps off it's least favorite student, student s is rejected. That means that the hospital favors $s\prime$ over s meaning $s\prime > s$. This contradicts our assumption and proves that hospital h's waitlist only improves with time.

Lemma: The algorithm must find a stable arrangement.

Let's suppose that our algorithm doesn't find a stable arrangement, and there's a rouge student hospital pair (s, h^*). (where s prefers h^* and vice-versa). Let's also say that s is now paired with h. For s to get paired with h, s must have had to propose to h^*, and since h^* prefers s, it would have not rejected s from it's waitlist. We have a contradiction here, proving that the algorithm does in fact find a stable arrangement.

Problem 4

$d = gcd(x, y) = ax + by$

(a) $d = gcd(x, y) = (a_0 + yk)x + (b_0 - xk)y$
$d = gcd(x, y) = a_0x + xyk + b_0y - xyk$
$d = gcd(x, y) = a_0x + b_0y$

$\forall k \ a = a_0 + yk, \ b = b_0 - xk$

(b) $gcd(30, 18) \rightarrow 30 = (1 \times 18) + 12$
$gcd(18, 12) \rightarrow 18 = (1 \times 12) + 6$
$gcd(12, 6) \rightarrow 12 = (2 \times 6) + 0$
$gcd(6, 0) \rightarrow 6 = (0 \times 0) + 6 \rightarrow \ m = 6$

extended gcd
$d = gcd(x, y) = \quad a_0x + b_0y$
$6 = gcd(6, 0) = \quad 1(6) + 0(0)$
$6 = gcd(12, 6) = \quad 0(12) + 1(6)$
$6 = gcd(18, 12) = \quad 1(18) - 1(6)$
$6 = gcd(30, 18) = -1(30) + 2(18) \rightarrow a_0 = -1, \ b_0 = 2$

$\forall k \ a = -1 + 18k, \ b = 2 - 30k$

(c) $d = gcd(x, y) = ax + by$
$2d = 2ax + 2by$
$2d = (2a)x + (2b)y$
$6 = gcd(30, 18) = -1(30) + 2(18)$
$2 \times 6 = (2 \times -1)(30) + (2 \times 2)(18)$
$12 = -2(30) + 4(18)$
$(a = -2, \ b = 4)$

Problem 5

(a) $(3002 + 6002 \times 9002) \bmod 3$
$(2 + 2 \times 2) \bmod 3$
$(2 + 4) \bmod 3$
$(6) \bmod 3$

$0 \bmod 3$

(b) $(1002^3 - 2468 \times 17 + 4) \bmod 5$
$(2^3 - 3 \times 2 + 4) \bmod 5$
$(8 - 6 + 4) \bmod 5$
$(3 - 1 + 4) \bmod 5$
$(6) \bmod 5$

$(1) \bmod 5$

(c) Inverses for $\{0, 1, 2, ..., 19\} \bmod 20$
$\gcd(20, 1) = \gcd(20, 3) = \gcd(20, 7) = \gcd(20, 9) = \gcd(20, 11) = \gcd(20, 13) = \gcd(20, 17) = \gcd(20, 19) = 1$

$\{1, 3, 7, 9, 11, 13, 17, 19\}$ have inverses mod 20

$1 = 1b \bmod 20$ *let* $b = 1$
$1 = 3b \bmod 20$ *let* $b = 7$
$1 = 7b \bmod 20$ *let* $b = 3$
$1 = 9b \bmod 20$ *let* $b = 9$
$1 = 11b \bmod 20$ *let* $b = 11$
$1 = 13b \bmod 20$ *let* $b = 17$
$1 = 17b \bmod 20$ *let* $b = 13$
$1 = 19b \bmod 20$ *let* $b = 19$

(d) $\dfrac{5-(19\times 3)}{7\times 9} \bmod 20$

$= \dfrac{5-57}{63} \bmod 20$

$= \dfrac{5+3}{3} \bmod 20$

$= \dfrac{8}{3} \bmod 20$

$= 8 \times 3^{-1} \bmod 20$

$= 8 \times 7 \bmod 20$ inverse found in 5c

$= 56 \bmod 20$

$= 16 \bmod 20$

(e) $1 = \gcd(m,x) = am + bx$

$\gcd(55, 36)$

$\gcd(55,36) \rightarrow 55 = 1(36) + 19$

$\gcd(36,19) \rightarrow 36 = 1(19) + 17$

$\gcd(19,17) \rightarrow 19 = 1(17) + 2$

$\gcd(17,2) \rightarrow 17 = 8(2) + 1$

$\gcd(2,1) \rightarrow 2 = 2(1) + 0$

$\gcd(1,0) \rightarrow 1 = 0(0) + 1$

Extended gcd for the inverse

$1 = \gcd(m,x) = am + bx$

$\gcd(1,0) = 1 = 1(1) + 0(0)$

$\gcd(2,1) = 1 = 0(2) + 1(1)$

$\gcd(17,2) = 1 = 1(17) - 8(2)$

$\gcd(19,17) = 1 = -8(19) + 9(17)$

$\gcd(36,19) = 1 = 9(36) + -17(19)$

$\gcd(55,36) = 1 = -17(55) + 26(36)$ $b = 26$

$36^{-1} \bmod 55 =$ **26**

$(26 \times 36) \bmod 55 = (936) \bmod 55 = (1) \bmod 55$ valid

(f) $17x \equiv 4 \bmod 20$

$(13) \times 17x \equiv (13) \times 4 \bmod 20$ inverse found in 5c

$x \equiv 52 \bmod 20$

$x \equiv 12 \bmod 20$

$\forall k \in \mathbb{Z}\ x = 12 + 20k$

(g) $5x + 3y \equiv 0 \pmod{19}$
$y \equiv 4 + 12x \pmod{19}$

$5x + 3y \equiv 0 \pmod{19} \rightarrow 3y \equiv -5x \pmod{19}$

$\rightarrow (-6) \times 3y \equiv (-6) \times -5x \pmod{19}$
$\rightarrow -18y \equiv 30x \pmod{19}$
$\rightarrow y \equiv 11x \pmod{19}$
$11x \equiv 4 + 12x \pmod{19}$
$0 \equiv 4 + x \pmod{19}$
$-4 \equiv x \pmod{19}$
$x \equiv 15 \pmod{19}$

$y \equiv 11(15) \pmod{19}$ Substitute x
$y \equiv 165 \pmod{19}$
$y \equiv 13 \pmod{19}$

$x \equiv 15 \pmod{19}$
$y \equiv 13 \pmod{19}$

Problem 6

(a) Prove $\{1a, 2a, ... \ (p-1)a\}$ where p is non-zero and $a \in \{1, 2..., \ p-1\}$ is a set of distinct numbers.

Lemma: Distinct integers
Let's assume that there are two products of some $x, y \in \{1, 2..., \ p-1\}$ and a such that they are modularly congruent for mod p.
$xa \equiv ya$ mod p
$x \equiv y$ mod p since a is non-zero and co-prime to p

We have a contradiction due to the fact that x, y are always less than $p-1$.
(x mod p $= x$) This would mean that $x = y$ which would state that the set is not distinct.
Proof by contradiction.

if we have $\{1a, 2a, ... \ (p-1)a\}$ then it's product would be $\prod_{i=1}^{p-1}(ai) = a^{p-1} \times \prod_{i=1}^{p-1}(i)$

From the previous lemma we showed that a set$\in \{1, 2, \ ... \ p-1\}$ has all distinct values and therefore has $p-1$ congruence classes. From this we can say that if an a is multiplied to all elements in the set then each element in $\{1, 2, \ ... \ p-1\}$ will be modularly congruent uniquely to some element in $\{1a, 2a, \ ... \ (p-1)a\}$ and therefore
$\prod_{i=1}^{p-1} i \equiv a^{p-1} \times \prod_{i=1}^{p-1}(i) \pmod{p}$

Due to the fact that Π is nonzero we can cancel it.

$1 \equiv a^{p-1}$ mod p Valid

(b) $\forall n$ S_n is the set of all integers $a \in \{1, 2, \ ... \ n-1\}$ such that $GCD(a, n) = 1$
This means that all integers in the set have to be coprime with n. If n is prime then $\{1, 2, \ ... \ n-1\}$ are all coprime with n and are in the set. $|S_n|$ denotes the number of coprime integers that are $(\leq n-1)$. Once again if n was prime then $|S_n|$ would be $n-1$.

Proof by Cases:

Case 1: n is prime

if n is prime then $|S_n|$ would be $n-1$ and we would have $a^{|S_n|} \equiv 1 \pmod{n}$
$a^{n-1} \equiv 1 \pmod{n}$ where $a \in \{1, 2, \ ... \ n-1\}$
We proved this in 6a. (Fermat's Little Theorem)

Case 2: n isn't prime

We can once again use the Lemma from 6a that proves that the integers in the set which are $(\leq n-1)$ are distinct. Since they are distinct, multiplying each number with a constant $\in S_n$ will result a modularly congruent set mod $(n-1)$.

Armed with the fact that the multiplying each element with an element in the set will result in the modularly equivalent set. We can state that the products are also modularly equivalent.

$$\prod_{i=1}^{|S_n|} S_i \equiv a^{|S_n|} \times \prod_{i=1}^{|S_n|} S_i \pmod{n}$$

Dividing both sides with Π which is obviously nonzero gives

$1 \equiv a^{|S_n|} \pmod{n}$ where $a \in S_n$ valid

Problem 7

(a) Base Case:
let $n = 1$
You can move the single largest disk from the source needle to the destination needle.
1 move.

let $n = 2$
You can move the smallest disk from the source needle to the buffer needle. Next move the largest disk to the destination needle. Now move the small disk on the buffer needle to the destination needle.
3 moves.

let $n = 3$
Move the smallest disk to the destination needle.
Next move the second largest disk to the buffer needle.
Now move the smallest disk on top of the buffer needle. ($n - 1$ on the buffer)
Now place the largest disk onto the destination needle.
Next place the smallest disk on the source needle.
The second largest onto the destination needle.
the smallest disk onto the destination needle.
7 moves.

From this we can see the strategy is to place $n-1$ disks onto a non-destination needle and then to place the n^{th} disk on the destination needle and then place $n-1$ on the destination needle. We need to continue this recursively until the base case is reached.
Since we are moving $n-1$ twice and $n = 1$ once we have
$F(n) = F(n-1) + F(1) + F(n-1) = 2F(n-1) + F(1) = 2F(n-1) + 1$

Now let's write out a table
$n = 4 \rightarrow \ F(4) = 2F(3) + 1 = 14 + 1 = 15$
$n = 5 \rightarrow \ F(5) = 2F(4) + 1 = 14 + 1 = 31$
$n = 6 \rightarrow \ F(6) = 2F(5) + 1 = 14 + 1 = 63$
$n = 7 \rightarrow \ F(7) = 2F(6) + 1 = 14 + 1 = 127$
From the table it looks like the pattern is $F(n) = 2^n - 1$

Proof: By induction on n
Inductive Hypotheis: $F(k) = 2F(k-1) + 1 = 2^k - 1$
let $n = k + 1$
$F(k+1) = 2F(k) + 1 = 2^{k+1} - 1$
$F(k+1) = 2(2^k - 1) + 1 = 2^{k+1} - 1$ Substitute inductive hypothesis
$F(k+1) = 2^{k+1} - 2 + 1 = 2^{k+1} - 1$
$F(k+1) = 2^{k+1} - 1 = 2^{k+1} - 1$
$F(k+1) = 2^{k+1}$ Valid

$2^{64} - 1 = 18446744073709551615$ seconds = 5.8 billion centuries