Brandon Vo

Assignment 3 CS-GY 6003

INET Spring 2021

Question 1: Recurrence Relations:

(50 points)

(a) Solve the following recurrence and prove your result is correct using induction:

$$a_1 = 1$$

$$a_2 = 3$$

$$a_n = a_{n-2} + 2^{\left\lfloor \frac{n}{2} \right\rfloor}$$

$$a_n - a_{n-2} - 2^{\left\lfloor \frac{n}{2} \right\rfloor} = 0$$

$$r^2 - 1 = 0$$

$$r = \pm 1$$

$$A_1 = 1$$

$$A_2 = 3$$

$$A_3 = A_1 - 2^{\left\lfloor \frac{3}{2} \right\rfloor} = 1 + 2^1 = 3$$

$$A_4 = A_2 - 2^{\left\lfloor \frac{4}{2} \right\rfloor} = 3 + 2^2 = 7$$

$$A_5 = A_3 - 2^{\left\lfloor \frac{5}{2} \right\rfloor} = (1 + 2^1) + 2^2 = 7$$

$$A_6 = A_4 - 2^{\left\lfloor \frac{6}{2} \right\rfloor} = (3 + 2^2) + 2^3 = 15$$

$$A_7 = A_5 - 2^{\left\lfloor \frac{7}{2} \right\rfloor} = (1 + 2^1 + 2^2) + 2^3 = 15$$

$$Closed\ form\ equation: = -1 + 2^{1+\left\lfloor \frac{n}{2} \right\rfloor}$$

Proof by Induction:

$$Base\ Case:\ a(1) = -1 + 2^{1+\left\lfloor \frac{1}{2} \right\rfloor}$$

$$a(1) = -1 + 2^{1+0} = 1, passes$$

$$a(2) = -1 + 2^{1+1} = -1 + 4 = 3, passes$$

Assume a(k) $= -1 + 2^{1+\left\lfloor \frac{n}{2} \right\rfloor}$

Must increment by 2 due to the floor function

$$a(2k) = -1 + 2^{1+\left\lfloor \frac{2k}{2} \right\rfloor}$$

Brandon Vo

$$a(2k) = -1 + 2^{\left\lfloor \frac{2k}{2} \right\rfloor} * 2$$

$$\boldsymbol{a(2k) = a(2k+1) = -1 + 2 * 2^{k}}$$

$$\boldsymbol{a(2k+2) = -1 + 2 * 2^{k+1}}$$

Brandon Vo

(b) Solve the following recurrence:

$$a_n + 9a_{n-1} - 108a_{n-3} = 0$$

$$a_n = -9a_{n-1} + 108a_{n-3}$$

$$a_0 = 9,\ a_1 = 9,\ a_2 = 243$$

$$r^3 + 9r^2 - 108 = 0$$

$$(r-3)(r+6)^2$$

$$r = 3, -6$$

$$a_n = a * 3^n + b * (-6)^n + nc * (-6)^n$$

$$n = 0, a * 3^0 + b * (-6)^0 = 9$$

$$a + b = 9$$

$$n = 1, a * 3^1 + b * (-6)^1 + 1 * c * (-6)^1 = 9$$

$$3a - 6b - 6c = 9$$

$$a - 2b - 2c = 3$$

$$n = 2, a * 3^2 + b * (-6)^2 + 2 * c * (-6)^2 = 243$$

$$9a + 36b + 72c = 243$$

$$a + 4b + 8c = 27$$

$$\boldsymbol{a = \frac{25}{3}, b = \frac{2}{3}, c = 2}$$

$$\mathbf{A_n = \frac{25}{3} * 3^n + \frac{2}{3} * (-6)^n + 2n * (-6)^n}$$

Closed form equation found

(c) There are n students competing in a school science fair. Each student can either compete on their own (individually) or by pairing up with someone else. Let T(n) be the number of ways for the students of the school to compete in the science fair. For example, if n = 3, then students 1, 2, 3 could compete as: {1}, {2}, {3} or {1, 2}, {3} or {1, 3}, {2} or {1}, {2, 3}, which is a total of 4 possibilities. Write a recurrence for T(n) including your base cases. Use the recurrence to solve for T(4), T(5) and T(6).

- The nth person can be either single or be paired with the rest of the n-1 people: Two cases of T(n-1) and T(n-2).
- If n is single, then T(n-1) is used. The extra person doesn't add anything. T(n-1) doesn't change.
- If n is being paired with the rest, then it must use the pairs of the T(n-2) because a second person adds another dimension to the list of paired groups. When the nth person is added, there are (n-1) people to pair the nth person with.

$$T(0) = 0$$

$$T(1) = \{1\} = 1$$

$$T(2) = \{1\}, \{2\}\ or\ \{\mathbf{1}, \mathbf{2}\} = 2$$

T(3) will use the set of T(2) but add 3 to each one.

$$T(3) = \{1\}\{2\}\{3\}\ or\ \{1,2\}\{3\}\ or\ \{\mathbf{1}, \mathbf{3}\}\{\mathbf{2}\}\ or\ \{\mathbf{1}\}\{\mathbf{2}, \mathbf{3}\}$$

(2+1) arrangements with 1 pair

$$T(3) = 1 + 3 = 4\ arrangements$$

$$T(4)\ uses\ the\ set\ of\ T(3)\ but\ adds\ a\ 4\ to\ each\ one$$

$$T(4) = \{1\}\{2\}\{3\}\{4\}\ or\ \{1, 2\}\{3\}\{4\}\ or\ \{1,3\}\{2\}\{4\}\ or\ \{\mathbf{1}, \mathbf{4}\}\{\mathbf{2}\}\{\mathbf{3}\}$$

$$or\ \{1\}\{2, 3\}\{4\}\ or\ \{\mathbf{1}\}\{\mathbf{2}, \mathbf{4}\}\{\mathbf{3}\}\ or\ \{\mathbf{1}\}\{\mathbf{2}\}\{\mathbf{3}, \mathbf{4}\}$$

3+3 arrangements with 1 pair

$$or\ \{\mathbf{1}, \mathbf{2}\}\{\mathbf{3}, \mathbf{4}\}\ or\ \{\mathbf{1}, \mathbf{3}\}\{\mathbf{2}, \mathbf{4}\}\ or\ \{\mathbf{1}, \mathbf{4}\}\{\mathbf{2}, \mathbf{3}\}$$

3 arrangements with 2 pairs

$$T(4) = 1 + 6 + 3 = 10\ arrangements$$

$$T(5) = \{1\}\{2\}\{3\}\{4\}\{5\}\ or\ \{1,2\}\{3\}\{4\}\{5\}\ or\ \{1, 3\}\{2\}\{4\}\{5\}\ or\ \{1,4\}\{2\}\{3\}\{5\}\ or\ \{\mathbf{1}, \mathbf{5}\}\{\mathbf{2}\}\{\mathbf{3}\}\{\mathbf{4}\}$$

$$\{1\}\{2, 3\}\{4\}\{5\}\ or\ \{1\}\{2, 4\}\{3\}\{5\}\ or\ \{\mathbf{1}\}\{\mathbf{2}, \mathbf{5}\}\{\mathbf{3}\}\{\mathbf{4}\}$$

$$\{1\}\{2\}\{3, 4\}\{5\}\ or\ \{\mathbf{1}\}\{\mathbf{2}\}\{\mathbf{3}, \mathbf{5}\}\{\mathbf{4}\}$$

$$or\ \{\mathbf{1}\}\{\mathbf{2}\}\{\mathbf{3}\}\{\mathbf{4}, \mathbf{5}\}$$

6+4 arrangements with one pair

$$\{1, 2\}\{3, 4\}\{5\}\ or\ \{\mathbf{1}, \mathbf{2}\}\{\mathbf{3}, \mathbf{5}\}\{\mathbf{4}\}\ or\ \{\mathbf{1}, \mathbf{2}\}\{\mathbf{3}\}\{\mathbf{4}, \mathbf{5}\}$$

$$\{1,3\}\{2,4\}\{5\}\ or\ \{\mathbf{1}, \mathbf{3}\}\{\mathbf{2}, \mathbf{5}\}\{\mathbf{4}\}\ or\ \{\mathbf{1}, \mathbf{3}\}\{\mathbf{2}\}\{\mathbf{4}, \mathbf{5}\}$$

$$\{1,4\}\{2,3\}\{5\}\ or\ \{\mathbf{1}, \mathbf{4}\}\{\mathbf{2}\}\{\mathbf{3}, \mathbf{5}\}\ \ or\ \{\mathbf{1}, \mathbf{4}\}\{\mathbf{2}, \mathbf{5}\}\{\mathbf{3}\}$$

Brandon Vo

$$\{\mathbf{1},\mathbf{5}\}\{\mathbf{2},\mathbf{3}\}\{\mathbf{4}\}\ or\ \{\mathbf{1},\mathbf{5}\}\{\mathbf{2},\mathbf{4}\}\{\mathbf{3}\}\ or\ \{\mathbf{1},\mathbf{5}\}\{\mathbf{3},\mathbf{4}\}\{\mathbf{2}\}$$

$$\{\mathbf{1}\}\{\mathbf{2},\mathbf{3}\}\{\mathbf{4},\mathbf{5}\}\ or\ \{\mathbf{1}\}\{\mathbf{2},\mathbf{4}\}\{\mathbf{3},\mathbf{5}\}\ or\ \{\mathbf{1}\}\{\mathbf{2},\mathbf{5}\}\{\mathbf{3},\mathbf{4}\}$$

3+12 arrangements with 2 pairs

$$T(5) = 1 + 10 + 15 = 26\ arrangements$$

Each paired set is incorporated into the set of the next one

$$T(n-1): The\ extra\ person\ added\ does\ not\ pair\ with\ anyone\ else.\ No\ change$$

$$T(n-2):\ The\ extra\ person\ is\ paired\ with\ someone.\ Has\ (n-1)\ choices\ of\ people\ to\ pair\ with.$$

$$Base\ Case:\ T(0) = T(1) = 1, T(2) = 2$$

$$\boldsymbol{T(n) = T(n-1) + T(n-2) * (n-1)}$$

$$T(3) = T(2) + T(1)(3-1) = 2 + 1 * 2 = 4$$

$$T(4) = T(3) + T(2)(4-1) = 4 + 2 * 3 = 10$$

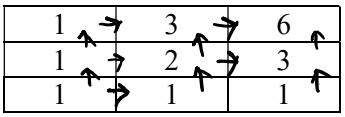
$$T(5) = T(4) + T(3) * (5-1) = 10 + 4 * 4 = 26$$

$$T(6) = T(5) + T(4) * (6-1) = 26 + 10 * 5 = 76$$

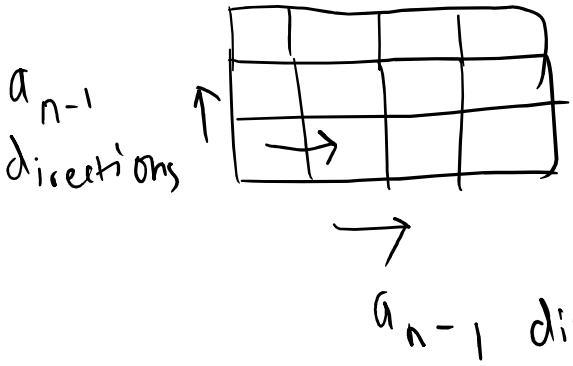
Brandon Vo

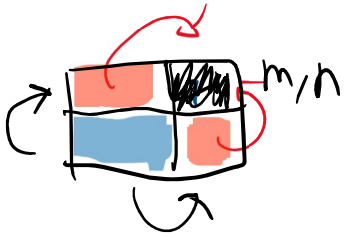
(d) A mouse is sitting in the bottom-left corner of an m × n chessboard. The mouse can move either right by one square or up by one square. The goal is to reach the cheese in the top right corner. Let M(m, n) be the number of different paths the mouse can take to reach the cheese. Write a recurrence for M(m, n), including the base cases. Solve the recurrence for m = 3, n = 3.

UU	UUR RUU URU	UURR URUR RRUU RURU 6 ways RUUR URRU
U	UR or RU	RRU RUR URR
X	R	RR



- Can move right one or up one





uses the 2 adjacent squares These red squares come from the blue square

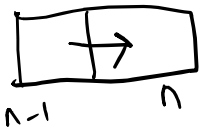
- Inclusion-Exclusion principle
- Go one direction, n - 1 ways to reach the destination
    - You can go on only in one direction at a time. Either up or right. Down and left are not allowed.
- Second case is adding one more possible direction on top of the previous results
- Base case has to be where $m \geq 1, n \geq 1$ *to allow for directions of up or down*

Brandon Vo

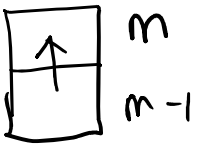
- When m=1 or n=1, then the case is always 1 because there is only one direction
- M(0,0) = 0

$$Base\ Cases:\ a(1,m) = a(n,1) = 1$$

$$\boldsymbol{a(n,m) = a(n-1,m) + a(n,m-1)}$$



$\boldsymbol{a(n-1,m)}$: *To the left of the destination. One way to go right.*



$\boldsymbol{a(n,m-1)}$: *Below the destination. One way to go up.*

$$\boldsymbol{a(3,3) = a(3,2) + a(2,3)}$$

$$\boldsymbol{a(3,3) = 3 + 3 = 6}$$

Brandon Vo

(e) Write a recurrence for the number of possible outcomes of flipping a coin n times such that there are no 3 heads in a row. You do not need to solve the recurrence.

- The only condition is no consecutive probability. 2 heads are fine.
- Order matters

$$C(n-1)\ for\ heads\ or\ tails$$

$$Must\ check\ the\ previous\ 2\ coin\ flips\ for\ heads\ then\ 1\ more\ coin\ flip\ for\ tails$$

$$C(0) = 1$$

$$C(1) = H, T = 2$$

$$C(2) = HH, HT, TH, TT = 4$$

$$C(3) = HHT, HTH, THH, HTT, THT, TTH, TTT = 7$$

$$C(3) = 1 + 2 + 4 = 7$$

C(4)= HHTH, HTHH, HHTT, HTHT, THHT, HTTH, THTH, TTHH, TTTH, TTHT, THTT, HTTT, TTTT = 13

$$C(4) = 2 + 4 + 7 = 13$$

C(5) = HHTHH, HHTTH, HTHTH, THHTH, HTTHH, HTHHT, THTHH, TTTHH, TTHTH, THTTH, TTHHT, THTHT, HTTHT, THHTT, HTHTT, HHTHT, HHTTT, TTTTH, TTTHT, TTHTT, THTTT, HTTTT, TTTTT = 24

$$C(5) = 13 + 7 + 4 = 24$$

$$First\ toss: 2\ scenarios$$

$$Two\ tosses: 2 * 2 = 4\ scenarios$$

$$Three\ tosses\ exclude\ HHH: 8 - 1 = 7\ scenarios$$

$$Every\ coin\ toss\ afterward\ is\ using\ a\ variation\ of\ these\ three\ cases$$

$$All\ cases\ of\ C(n)\ must\ be\ disjointed.$$

After every coin toss of C(n-1), you can only toss a coin another time for C(n-2). After C(n-2), you can only toss the coin again for C(n-3). This only changes the base cases. Each coin toss of C(n-1) and further adds only T or H. C(n-1) cannot affect C(n-2) or C(n-3) because they have to be disjointed sets. There is no extra option for a coin toss except for not including the cases for consecutive heads to begin with.

$$C(n-1):\ Flip\ a\ coin\ once$$

$$C(n-2):\ Flip\ a\ coin\ a\ second\ time$$

$$C(n-3):\ Flip\ a\ coin\ a\ third\ time$$

$$\boldsymbol{C(n) = C(n-1) + C(n-2) + C(n-3)}$$

Brandon Vo

(f) Let g(n) : N → N where g(n) = n^2 + n. Express g(n) as a recurrence.

$$g(n) = n(n+1)$$

$$g(0) = 0$$

$$g(1) = 1(1+1) = 1 * 2 = 2$$

$$g(2) = 2(2+1) = 2 * 3 = 2 * \mathbf{3} = 6$$

$$g(3) = 3(3+1) = 3 * 4 = 6 * \mathbf{2} = 12$$

$$g(4) = 4(4+1) = 4 * 5 = 12 * \frac{\mathbf{5}}{\mathbf{3}} = 20$$

$$g(n)\ uses\ one\ previous\ case:\ g(n-1)$$

$$g(n)\ uses\ multiplicative\ relationship\ with\ its\ previous\ cases.\ The\ pattern\ shows\ that\ it's\ based\ off\ n.$$

$$Working\ backwards\ from\ g(4), \frac{5}{3}\ can\ also\ be\ shown\ as \frac{4+1}{3}, grabbing\ the\ 3\ from\ g(3)'s\ n$$

$$g(3)\ uses\ 2\ or \frac{3+1}{2}, grabbing\ the\ 2\ from\ g(2)'s\ n$$

$$g(2)\ uses\ 3\ or \frac{3}{1}, taking\ the\ 1\ from\ n$$

$$g(2) = 2(2+1) = 2 * 3 = 2 * \frac{\mathbf{3}}{\mathbf{1}} = 6$$

$$g(3) = 3(3+1) = 3 * 4 = 6 * \frac{\mathbf{4}}{\mathbf{2}} = 12$$

$$g(4) = 4(4+1) = 4 * 5 = 12 * \frac{\mathbf{5}}{\mathbf{3}} = 20$$

$$The\ fraction\ has\ a\ difference\ of\ two, but\ they\ are\ both\ incrementing\ by\ 1\ each\ time: \frac{n+1}{n-1}$$

$$g(n) = g(n-1) * \frac{n+1}{n-1}$$

$$g(2) = g(1) * \frac{3}{1} = 2 * 3 = 6$$

$$g(3) = g(2) * \frac{4}{2} = 6 * 2 = 12$$

$$g(4) = g(3) * \frac{5}{3} = 12 * \frac{5}{3} = 20$$

$$\boldsymbol{g(n) = g(n-1) * \frac{n+1}{n-1}}\ \text{where n} \geq 2 \text{ and g(1)} = 2$$

Brandon Vo

$$Induction:$$

$$Base\ case:\ g(2) = g(1) * \frac{3}{1} = 2 * 3 = 6$$

$$g(k) = g(k-1) * \frac{k+1}{k-1}$$

$$g(k) = k^2 + k$$

$$Induction\ Step:\ g(k+1) = g(k) * \frac{k+2}{k} = (k^2 + k) * \frac{k+2}{k}$$

$$g(k+1) = (\boldsymbol{k+1}) * (\boldsymbol{k+2})$$

$$g(k+1) = \boldsymbol{k^2 + 3k + 2}$$

$$g(k+1) = (k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = \boldsymbol{k^2 + 3k + 2}$$

Compared to the original n equation:

$$g(n) = n^2 + n$$

$$(n+1)^2 + n + 1 = (n+3)(n+2)$$

(g) A construction worker is tiling a pathway into a newly built home. The pathway has length n. There are black stones of length 1, brown and white stones of length 2, and grey stones of length 3. The worker places the stones one after the other to create a patterned walkway. Let W(n) be the number of ways to tile a pathway of length n using these stones. Write a recurrence W(n), including the base cases. Suppose that the neighbor requests a similar walkway but doesn't want two stones of size 2 adjacent to each other. Write a new recurrence for the number of different possible for the neighbor. Include your base cases. You do not need to solve the recurrence.

- Anytime a size 2 stone is laid down, it must be followed by a size 1 or size 3 stone
- There are 2 types of size 2 stones
- Order matters

$$The\ original\ conditions\ (with\ adjacent\ stones\ allowed):$$

$$W(n) = W(n-1) + 2W(n-2) + W(n-3)$$

With the neighbor's conditions

$$Base\ Cases:\ W(0), W(1), W(2), W(3), W(4)$$

$$W(0) = 1\ (no\ blocks)$$

$$W(1) = B = \mathbf{1\ arrangement}$$

$$W(2) = BB, W, R = 1 + 1 * 2 = \mathbf{3\ arrangements}$$

$$W(3) = BBB, BW, WB, BR, RB, G = 1 + 2 * 2 + 1 = \mathbf{6\ arrangements}$$

$$W(4) = BBBB, BBW, BWB, WBB, BBR, BRB, RBB, GB, BG$$

$$W(4) = 1 + 2 * 3 + 2 = \mathbf{9\ arrangements}$$

W(5) = BBBBB, BBBW, BBWB, BWBB, WBBB, BBBR, BBRB, BRBB, RBBB, WBW, RBW, RBR, WBR, BBG, BGB, GBB, GW, WG, GR, RG

$$W(5) = 1 + 2 * 4 + 2 * 2 + 3 + 2 * 2 = \mathbf{20\ arrangements}$$

W(6) = BBBBBB, BBBBW, BBBWB, BBWBB, BWBBB, WBBBB, BBBBR, BBBRB, BBRBB, BRBBB, RBBBB, WBWB, WBBW, BWBW, BWBR, WBRB, RBWB, WBBR, RBBW, RBBR, BRBR, RBRB, BBBG, BBGB, BGBB, GBBB, WGB, WBG, BWG, BGW, GBW, GWB, RGB, RBG, BRG, BGR, GBR, GRB, GG

$$W(6) = \mathbf{39\ arrangements}$$

$$W(6) = W(5) + W(4) + W(2) + W(1) + W(3) = 20 + 9 + 6 + 3 + 1 = 39$$

$$W(5) = W(4) + W(3) + W(1) + W(0) + W(2) = 9 + 6 + 3 + 1 + 1 = 20$$

Brandon Vo

$$W(n-1)\ just\ means\ an\ additional\ black\ stone, no\ change$$

$$W(n-3)\ means\ an\ additional\ grey\ stone, no\ change$$

$$2W(n-2)\ was\ originally\ the\ case\ due\ to\ having\ two\ choices\ of stones\ to\ choose.$$

$$W(n-1), W(n-2), and\ W(n-3)\ are\ disjointed\ sets.\ One\ set\ does\ not\ affect\ the\ other.$$

However, the neighbor's floor tile affects 2W(n-2). Because of the adjacency requirement, that means W(n-2) must be followed by a black or grey tile, changing the W(n-2) case. This requires looking at what is behind W(n-2) which could be W(n-4) and W(n-5).

$$W(n-2)\ must\ now\ check\ for\ adjacency, requiring\ additional\ base\ cases$$

$$\boldsymbol{W(n) = W(n-1) + W(n-2) + W(n-4) + W(n-5) + W(n-3)}$$

$$\boldsymbol{Base\ Cases}:\ W(0), W(1), W(2), W(3), W(4)$$

$$W(0) = W(1) = 1$$

$$W(2) = 3$$

$$W(3) = 6$$

$$W(4) = 9$$

Brandon Vo

Question 2

a) Let p = 683 and q = 577. Show how to create public and private keys of RSA encryption using these two primes. Encode the message m = 100 and show how it is successfully decoded.

$$n = pq = 394091$$

$$m = (p-1)(q-1) = 682 * 576 = 392832$$

$$Choosing\ numbers\ e\ and\ d\ so\ that\ e * d\ has\ a\ remainder\ of\ 1\ when\ divided\ by\ m$$

$$e = 8017, d = 49$$

$$8017 * 49 = 392833\ mod\ 392832 = 1$$

$$\boldsymbol{(n, e) = (394091, 8017), this\ is\ the\ public\ key}$$

The private key will use the same n, but will use d for factoring

$$\boldsymbol{(n, d) = (394091, 49), this\ is\ the\ private\ key}$$

$$Encrypting\ M = 100$$

$$M^e\ mod\ n = C$$

$$100^{8017}\ mod\ 394091 = 170264$$

$$\boldsymbol{C = 170264, the\ cipher\ text\ which\ is\ sent\ out}$$

$$Decoding\ C = 170264$$

$$M = C^d\ mod\ n$$

$$Going\ to\ use\ the\ private\ key\ (n, d)\ |\ (394091, 49)$$

$$\boldsymbol{170264^{49}\ mod\ 394091\ = 100\ which\ is\ the\ original\ message}$$

Brandon Vo

b) Suppose Jeff would like to receive a message from John using RSA encryption. Jeff selects two primes, determines that n = 3953 and selects a public key e = 19. In preparing to send the information to John, he sends n correctly but accidentally leans on his calculator before sending e, and sends off 19^2 in the place of e. John encrypts his message using the keys that he receives, not knowing that there is an error in the public key e. Jeff receives the message s = 138. How can he decode it using the private key d = 403? Explain why your solution is correct.

$$(3953, 19):\ Original\ public\ key$$

$$(3953, 403):\ Private\ key$$

$$p = 59, q = 67$$

$$r = (p-1)(q-1) = 58 * 66 = 3828$$

Using 7657 as the relative prime

$$7657 = 19 * 401, e = 19, d = 403$$

The encryption with the mistake

$$m^{19^2}\ mod\ 3953 = 138$$

Must find a way to factor m.

$$s = m^e mod\ n, m' = c^d mod\ n; s = m^d mod\ n, s' = s^e mod\ n$$

$$138 = m^{19^2}\ mod\ 3953$$

$$m = c^{403^n} mod\ 3953$$

$$To\ decrypt\ using\ d = 403:\ square\ 403\ as\ well$$

$$Original\ decryption:\ 138^{403}\ mod\ 3953 = m$$

$$138^{403^2}\ mod\ 3953 = m$$

$$m = 100$$

$$Testing:\ 100^{19^2} mod\ 3953 = 138$$

$$GCD(361, 403) = 1$$

$$138^{403^2} mod\ 3953 = 1$$

$$s = m^e\ mod\ n$$

$$m = s^d\ mod\ n$$

$$m = (m^e)^d\ mod\ n$$

$$m = m^{ed}\ mod\ n$$

Brandon Vo

$$m = m^{19*403} mod\ 3953$$

e and d must be inverses of mod n for RSA encryption to work

$$403 * 19\ mod\ 3828 = 1, these\ two\ can\ be\ used\ as\ inverses$$

$$403^2 * 19^2\ mod\ 3828 = 1$$

$$(403 * 19)\ (403 * 19)\ mod\ 3953$$

$$1 * 1\ mod\ 3828, 403^2\ and\ 19^2\ are\ still\ inverses\ of\ n$$

$$RSA\ Encryption:\ m = m^{ed} mod\ n$$

$$m^{e*d^2}\ mod\ n\ \neq m$$

$$m^{(ed)^2} mod\ n = m^{ed} * m^{ed}\ mod\ n$$

$$m^{ed} * m^{ed} mod\ n = m$$

19 and 403 are still relatively prime numbers and inverses for n. 19^2 and 403^2 still leaves 19 and 403 as the inverses, making the cipher still valid due to mod n. RSA encryption and the (p-1)(q-1) method is used to find two relatively prime numbers and inverses to serve as the public and private key.

RSA encryption is designed so that multiple public keys can be used and decoded by one private key as long as the public and private keys are relatively prime.

c) Recall the problem of Jeff and John from above. The next day, Jeff decides he can do better. Jeff is determined to send the correct information! Using the same primes, he computes n = 3953 and e = 19 and d = 403. He sends off the values 3953 and 403 to John. John receives these keys and doesn't know there is an error in the public key. Again! He encodes his message and sends it off. Jeff receives the message s = 3885. Explain how Jeff can decode this message, even though it was encoded with the private key. What does this work?

Same public and private key intentions as before.

$$(3953, 19):\ Original\ public\ key$$

$$(3953, 403):\ Private\ key$$

$$p = 59, q = 67$$

$$r = (p-1)(q-1) = 58 * 66 = 3828$$

Using 7657 as the relative prime

$$7657 = 19 * 401, e = 19, d = 403$$

$$m^{403} = 3885\ mod\ 3953$$

If 403 was send as the public key, that still leaves 19 as an available inverse. 19 can just be used as the private key instead.

$$3885^{19}\ mod\ 3953 = m$$

$$m = 200$$

$$Testing: 200^{403} mod\ 3953 = 3885$$

$$3885^{19} mod\ 3953 = 200$$

$$RSA\ Encryption:\ m = m^{ed}\ mod\ n$$

- Because RSA encryption works essentially as $m = m^{ed}$ mod n, e and d can be used interchangeably as long as they're inverses of n.

19 and 401 are chosen as the keys because they're relatively prime and are used as inverses for mod n. As a result, either key can be chosen as the public or private key because e and d are inverses for each other. If d was sent out as the public key, e is still available to decode d because e is the inverse for d.

Brandon Vo

d) Solve the equation below for x, y ∈ Z using the extended Euclidean algorithm:

$$ax + by = GCD(a, b)$$

43845x + 342y = 9

GCD(43845, 342) = 3

$$14615x + 114y = 3$$

$$Euclid's\ algorithm$$

$$14615 = 114 * 128 + 23$$

$$114 = 23 * 4 + 22$$

$$23 = 22 * 1 + 1$$

$$69 = 43845 - 114 * 384$$

$$45 = 114 - 69 * 1$$

$$24 = 69 - 45 * 1$$

$$21 = 45 - 24 * 1$$

$$3 = 24 - 21 * 1$$

Substitute every number back up until we get only factors of 43845 and 114

$$3 = 24 - 21(1) = 24 - (45 - 24)$$

$$3 = (69 - 45) - (45 - 24)$$

$$3 = \big(43845 - 114(384) - (114 - 69)\big) - \big((114 - 69) - (69 - 45)\big)$$

$$3 = \big(43845 - 114(384) - (114 - 69)\big) - \big((114 - 69) - ((43845 - 114 * 384) - (114 - 69))\big)$$

$$3 = (43845 - 114(385) + (43845 - 114 * 384)) - \big((114 - (43845 - 114 * 384)) - \big((43845 - 114 * 385) + 69\big)\big)$$

$$3 = \big(43845(2) - 114(769)\big) - \big((-(43845 - 114 * 385) - \big((43845 - 114 * 385) + 69\big)\big)$$

$$3 = \big(43845(2) - 114(769)\big) + \big(43845 - 114 * 385 + \big((43845 - 114 * 385) + 69\big)\big)$$

$$3 = \big(43845(3) - 114(1154)\big) + \big((43845 - 114 * 385) + 69\big)$$

$$3 = \big(43845(4) - 114(1539)\big) + 69$$

$$3 = 43845(4) - 114(1539) + 43845 - 114 * 384$$

$$3 = 43845(5) - 114(1923)$$

Brandon Vo

$$To\ have\ it = 9, multiple\ everything\ by\ 3$$

$$\mathbf{9 = 43845(15) - 342(1923)}$$

Brandon Vo

e) Use number theory to explain why can't make any amount of postage over k cents using 6 and 27 cent stamps. Use number theory to explain why we can make any postage of at least 12 cents using 4 and 5 cent stamps. (Hint: consider the division algorithm where d = 4).

$$x = k \ mod \ 6$$

$$x = k \ mod \ 27$$

$$GCD(6, 27) = 3$$

These two are not relative prime numbers, they can only divide postage stamps that are multiples of 3

Proof by cases: Show for 6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5

$$54 = 6q \ mod \ 27$$

$$0 = 6q \ mod \ 27$$

$$\boldsymbol{q = 0}$$

$$55 = 6q \ mod \ 27$$

$$1 = 6q \ mod \ 27$$

$6 \ mod \ 27$ *does not have an inverse*: ***No possible solution***

$$56 = 6q \ mod \ 27$$

$$2 = 6q \ mod \ 27$$

$$2 = 6q \ mod \ 27$$

No value for q available (**2 *is not a multiple of* 3**)

$$57 = 6q \ mod \ 27$$

$$3 = 6q \ mod \ 27$$

$$30 = 6q \ mod \ 27$$

$$q = \ 5 \ mod \ 27$$

$$\boldsymbol{q = 5}$$

$$58 = 6q \ mod \ 27$$

$$4 = 6q \ mod \ 27$$

No value of q possible (**4 *is not a multiple of* 3**)

$$59 = 6q \ mod \ 27$$

$$5 = 6q \ mod \ 27$$

No value of q possible (**5 *is not a multiple of* 3**)

Brandon Vo

$$6x\text{: } 6, 12, \dots, 24, 30, 36, 42, 48, \mathbf{54}, 60, 66, 72, 78, 84, 90, 96, 102, \mathbf{108}, \dots$$

$$27x\text{: } 27, \mathbf{54}, 81, \mathbf{108}, 135, 162, 189 \dots.$$

6 and 27 are not relatively prime, meaning that the values they can handle must be within the range of their GCD value which is 3. Postage stamps of 6 and 27 can only handle total values that are also a multiple of 3. If not, then there isn't a method to handle the total postage stamp value.

$$Division\ algorithm\text{: } n = q * d + r$$

$$See\ how\ we\ can\ make\ n = 4k, 4k+1, 4k+2, 4k+3$$

$$12 = 4q\ mod\ 5$$

$$\boldsymbol{q = 3}$$

$$13 = 4q\ mod\ 5$$

$$3 = 4q\ mod\ 5$$

$$-2 = -q\ mod\ 5$$

$$\boldsymbol{q = 2}$$

$$14 = 4q\ mod\ 5$$

$$4 = 4q\ mod\ 5$$

$$\boldsymbol{q = 1}$$

$$15 = 4q\ mod\ 5$$

$$0 = 4q\ mod\ 5,$$

$$\boldsymbol{q = 0}$$

$$16 = 4q\ mod\ 5$$

$$\boldsymbol{q = 4}$$

Brandon Vo

There are different q values for 4k mod 5 where the values of k are values from 12 to 16. This shows that the values of 4 will end up as a value that either divides the total postage stamp or leaves a remainder that is divisible by 5. This is because 4 and 5 are relatively prime. Their GCD value is 1.

Brandon Vo

f) Solve $x^3 - 4x^2 + 8x = 0 \bmod 16$. There are four solutions.

$$Factors\ of\ 16\ can\ be\ 2^4$$

$$Split\ the\ equation\ into\ mod\ 2 * mod\ 8$$

$$x(x^2 - 4x + 8) = 0\ mod\ 8$$

Completing the square under mod 8

$$x(x^2 - 4x + 4) + 4x = 0\ mod\ 8$$

$On\ the\ LHS, using\ any\ multiple\ of\ 4\ would\ result\ in\ two\ numbers\ that\ are\ a\ multiple\ of\ 4\ adding\ up$

The result shows that any number of x that is a multiple of 4 would end up as a multiple of 16

$$x(x+1)^2 - 2x^2 - 9x = 0\ mod\ 16$$

$$x^3 - 4x^2 + 8x = 0\ mod\ 8$$

$$x^3 - 4x^2 = 0\ mod\ 8$$

$$x^2(x-4) = 0\ mod\ 8$$

$$\boldsymbol{x = 0, 4}$$

$$x = 4\ mod\ 8 \equiv 12$$

$$x = 12$$

$$x^3 - 4x^2 + 8x = 0\ mod\ 16$$

$$x^3 - 4x^2 - 8x = 0\ mod\ 16$$

$$x^3 - 4x^2 = 8x\ mod\ 16$$

$$x(x^2 - 4x) = 8x\ mod 16$$

$$x^3 - 4x^2 = 8x\ mod\ 16$$

$$x(x-4) = 8\ mod\ 16$$

$$\boldsymbol{x = 0, 8}$$

$$x^3 - 4x^2 + 8x = 0\ mod\ 16$$

$$x(x-2)^2 - 4x = 0\ mod\ 16$$

$$x(x-2)^2 = 4x\ mod\ 16$$

Brandon Vo

$$x = 0, 4, 8, 12$$

$$(x-2)^2 = 4 \; mod \; 16$$

$$x - 2 = 2 \; mod \; 16$$

$$\boldsymbol{x = 4}$$

$$x^3 - 4x^2 + 8x = 0 \; mod \; 8$$

$$x^3 + 4x^2 = 0 \; mod \; 8$$

$$x^2(x+4) = 0 \; mod \; 8 \, , x = 0, -4$$

$$\boldsymbol{x = 0, 12}$$

$$x = 4, 8, 12$$

x = 0	0
x = 4	48 mod 16 = 0
x = 8	416 mod 16 = 0
x = 12	1488 mod 16 = 0

Brandon Vo

g) For each of the following, solve for x or prove that there is no solution:

- 6x = 2 mod 48

$$Possible\ values\colon\ 6, 12, 18, 24, 30, 36, 42, 48, 6 \ldots$$

$$Because\ 6\ is\ a\ factor\ of\ 48, only\ the\ factors\ above\ are\ available\ for\ x.$$

GCD(6, 48) = 8. 8 is not a factor of 2. An inverse does not exist for this equation. There is no solution.

- 5x = 2 mod 48

GCD(5, 48) = 1. 1 is a factor of 2. Solution exists.

Inverse of 5 is 29 because 29*5 = 145. 145 mod 48 = 1

$$5x * 29 = 2 * 29\ mod\ 48$$

$$5x * 29 = 58\ mod\ 48$$

$$145x = 58\ mod\ 48$$

$$x = 58\ mod\ 48$$

$$\boldsymbol{x = 10\ mod\ 48}$$

- 10x = 2 mod 48

  GCD(10, 2) = 2. 2 is a factor of 48. Solution exists.

  Equivalent of solving 5x = 1 mod 24

$$Inverse\ of\ 5\ is\ 5\ because\ 25\ mod\ 24\ is\ 1$$

$$5x * 5 = 1 * 5\ mod\ 24$$

$$25x = 5\ mod\ 24$$

$$x = 5\ mod\ 24$$

$$\boldsymbol{x = 5\ mod\ 48}$$

- 10x = 0 mod 48

GCD(10, 0) = 0

$$X = 0\ is\ the\ only\ solution\ available$$

Brandon Vo

h) Evaluate the following using the theorems and definitions from class

- 7^{663} mod 67

Fermat's Little Theorem

$$a^{p-1} \equiv 1 \; mod \; p \; if \; a \; and \; p \; are \; relatively \; prime$$

$$a = 7, p = 67$$

$$p - 1 = 66$$

$$7^{66} \equiv 1 \; mod \; 67$$

$$7^{(66)10} * 7^3 = 7^{663}$$

$$7^3 \; mod \; 67 = 8$$

$$\boldsymbol{7^{663} mod \; 67 = 8}$$

- 134^{160} mod 17

$$Fermat's \; Little \; Theorem$$

$$a^{p-1} \equiv 1 \; mod \; p \; if \; a \; and \; p \; are \; relatively \; prime$$

$$a = 134, p = 17$$

$$p - 1 = 16$$

$$134^{16} \equiv 1 \; mod \; 17$$

$$134^{8} \equiv 1 \; mod \; 17$$

$$134^{(8)20} \equiv 1 \; mod \; 17$$

$$\boldsymbol{134^{160} \; mod \; 17 = 1}$$

- 134^{160} mod 67

GCD(134, 67) = 67

The entire 134^{160} is factored by 67.

$$134 \; mod \; 67 = 0$$

$$\boldsymbol{134^{160} mod \; 67 = 0}$$