Homework 3: Name Bingying Liang ID 48999397

1. [15 pts] Given you have three dice where die D1 has faces $\{0, 2, 2, 2, 3, 3\}$ die D2 has faces $\{2, 3, 3, 5\}$ and Die D3 has faces $\{2, 2, 2, 1, 1, 1, 0, 0\}$. Fill in the dynamic programming table for D1 and D2 and D3.

   (i) Indicate how many different ways you can roll the value 7 using all the three dice in the problem.

   Solution: 45

   (ii) Indicate how many different ways you can roll the value 11 using all three dice in the problem.

   Solution: 0. Because Max face of D1, D2, D3 are 3,5,2 and then $3+5+2 = 10 < 11$.

   (iii) What is the Probability of rolling a 7?

   Solution:

$$\frac{42}{6 \times 4 \times 8} = \frac{42}{192} = \frac{7}{32}$$

die sum	D1 (ways)	D1+D2 (ways)	D1+D2+D3 (ways)
0	1	0	0
1	0	0	0
2	3	1	2
3	2	2	7
4	0	3	15
5	0	9	33
6	0	4	44
7	0	3	45
8	0	2	25
9	0	0	15
10	0	0	6
11	0	0	0
Sum ways	6	24	192

2. [15 pts] You have 4 items to consider:

   - Item 1 weighs 1 lb and is worth \$2.
   - Item 2 weighs 5 lbs and is worth \$7.
   - Item 3 weighs 6 lbs and is worth \$8.
   - Item 4 weighs 2 lbs and is worth \$3.

   (i) If you can carry 11 lbs and can not divide the items. There is also only one of each item available. Set up the table to show which items you would take.

Solution:

Carry weight	Value from item 1	Value from item 1 and 2	Value from item 1 to 3	Value from item 1 to 4
0	0	0	0	0
1	2	2	2	2
2	2	2	2	3
3	2	2	2	5
4	2	2	2	5
5	2	7	7	7
6	2	9	9	9
7	2	9	10	10
8	2	9	10	12
9	2	9	10	13
10	2	9	10	13
11	2	9	15	15
12	2	9	17	17
13	2	9	17	18
14	2	9	17	20

Therefore, if I can carry 11 lbs, I will take item2, item3 and the value of them is $15.

(ii) Assume you can divide the items. That is 25% of an item weighs 25% as much and is worth 25% of the value. You can take a maximum of 100% of an item. That is there is only one of each item available. Which items would you take and how much of each item would you take?

Solution:

Item	1	2	3	4
Weight	1	5	6	2
Worth	2	7	8	3
Ratio $(\frac{Worth}{Weight})$	2	1.4	$\frac{8}{6}$	1.5

Carry weight	Value from item 1	Value from item 1 and 4	Value from item 1, 4, 2	Value from item 1, 4, 2, 3
0	0	0	0	0
1	2	2	2	2
2	2	3.5	3.5	3.5
3	2	5	5	5
4	2	5	6.4	6.4
5	2	5	7.8	7.8
6	2	5	9.2	9.2
7	2	5	10.6	10.6
8	2	5	12	12
9	2	5	12	$\frac{40}{3} \approx 13.33$
10	2	5	12	$\frac{44}{3} \approx 14.67$
11	2	5	12	16
12	2	5	12	$\frac{52}{3} \approx 17.33$
13	2	5	12	$\frac{56}{3} \approx 18.67$
14	2	5	12	20

According to the ratio, I take the item 1 first, then item 4, then item 2, then item 3 Therefore, if I can carry 11 lbs, I will take 100% item1, 100% item4, 100% item2, 50% item3 and the value of them is $\$16$.

3. [10 pts] A table was created and filled in for determining the Longest Increasing Subsequence. The final row of the table is shown below.

1	2	4	5	6	8

(i) What does the value 6 indicate?

Solution: The 5th value of the longest Increasing subsequence is 6.

(i) What does the value 5 indicate?

Solution: The 4th value of the longest Increasing subsequence is 5.

(i) How long is the Longest Increasing Subsequence?

Solution: 6

4. [10 pts] Set up a table and show the Longest Common Subsequence for the following two strings:

A A C C T C G T A C and A C C A T G G T A A C T

(You may do this in Excel and show your results here)

Solution:

	-	A	A	C	C	T	C	G	T	A	C
-	0	0	0	0	0	0	0	0	0	0	0
A	0	1	1	1	1	1	1	1	1	1	1
C	0	1	1	2	2	2	2	2	2	2	2
C	0	1	1	2	3	3	3	3	3	3	3
A	0	1	1	2	3	3	3	3	3	4	4
T	0	1	1	2	3	4	4	4	4	4	4
G	0	1	1	2	3	4	4	5	5	5	5
G	0	1	1	2	3	4	4	5	5	5	5
T	0	1	1	2	3	4	4	5	6	6	6
A	0	1	2	2	3	4	4	5	6	7	7
A	0	1	2	2	3	4	4	5	6	7	7
C	0	1	2	3	3	4	5	5	6	7	8
T	0	1	2	3	3	4	5	5	6	7	8

The longest Common Subsequence is “ACCTGTAC” and its length is 8.

5. [10 pts] Show the table to find the Levensthein Edit Distance of the following two strings: What is the edit distance?

A C T G T A C G C and A T X T C G C Y M

(You may do this in Excel and show your results here)

Solution:

	-	A	C	T	G	T	A	C	G	C
-	0	1	2	3	4	5	6	7	8	9
A	1	0	1	2	3	4	5	6	7	8
T	2	1	1	1	2	3	4	5	6	7
X	3	2	2	2	2	3	4	5	6	7
T	4	3	3	2	3	2	3	4	5	6
C	5	4	3	3	3	3	3	3	4	5
G	6	5	4	4	3	4	4	4	3	4
C	7	6	5	5	4	4	5	4	4	3
Y	8	7	6	6	5	5	5	5	5	4
M	9	8	7	7	6	6	6	6	6	5

ACTGTACGC → ATGTACGC (delete “C”)
ATGTACGC → ATXTACGC (replace “G” with “X”)

ATXTACGC $\rightarrow$ ATXTCGC (delete "A")
ATXTCGC $\rightarrow$ ATXTCGCY (insert "Y")
ATXTCGCY $\rightarrow$ ATXTCGCYM (insert "M")

6. [10 pts] Consider two strings. The length of the first string is unknown and the length of the second string is fifteen. The Levensthein edit distance between the strings is 6.

   a. What is the maximum possible length of the first string?

      Solution: 21

   b. What is the minimum possible length of the first string?

      Solution: 9

   c. What is the maximum possible length of the Longest Common Subsequence of the two strings?

      Solution: 15

   d. What is the minimum possible length of the Longest Common Subsequence of the two strings?

      Solution: 9

7. [10 pts] Set up the table for the Extended Euclidian Algorithm and use it to find

$$1/19 \text{ modulo } 3315$$

Solution:

	A	B	Q	R	α	β
-1					1	0
0	3315	19	174	9	0	1
1	19	9	2	1	1	-174
2	9	1	9	0	-2	349
3	1	0	-	-	19	3315

$$-2 \times 3315 + 19 \times 349 = 1$$
$$(-2 \times 3315) \,\%\, 3315 + (19 \times 349) \,\%\, 3315 = 1 \,\%\, 3315$$
$$0 + (19 \times 349) \,\%\, 3315 = 1$$
$$\therefore (19 \times 349) \,\%\, 3315 = 1$$
$$(19 \times \frac{1}{19}) \,\%\, 3315 = 1$$
$$\therefore \frac{1}{19} \,\%\, 3315 = 349$$

8. [20 pts] Bob encoded a message to Alice using RSA. Alice's public key is $e = 82313$ with a modulus of 467807. Using a quantum computer, you were able to factor the modulus into the product of two primes, $677 * 691$. Assumes the cipher text is 2.

   a. What is Alice's Private Key (show your table for calculating the Extended Euclidian Algorithm)

   Solution:

$$n = 467807 = (pq) = 677 \times 691$$
$$\phi(n) = (p-1)(q-1) = 676 \times 690 = 466440$$
$$d = \frac{1}{e} \,\%\, \phi(n) = \frac{1}{82313} \,\%\, 466440$$

	A	B	Q	R	α	β
-1					1	0
0	466440	82313	5	54875	0	1
1	82313	54875	1	27438	1	-5
2	54875	27438	1	27437	-1	6
3	27438	27437	1	1	2	-11
4	27437	1	27437	0	-3	17
5	1	0	-	-	82313	-466440

$$-3 \times 466440 + 17 \times 82313 = 1$$
$$(-3 \times 466440) \,\%466440 \; + (17 \times 82313) \,\%\, 466440 = 1 \,\%\, (466440)$$
$$0 + (17 \times 82313) \,\%\, 466440 = 1$$
$$\therefore (17 \times 82313) \,\%\, 466440 = 1$$
$$\because (\frac{1}{82313} \times 82313) \,\%\, 466440 = 1$$
$$\therefore (\frac{1}{82313}) \,\%\, 466440 = 17$$
$$\therefore d = 6$$
$$\therefore \text{Alice's Private Key is } \{17, 467807\}$$

   b. What was the un-encrypted message Bob was sending to Alice?

   Solution:

$$\because c = 2$$
$$\therefore 2^{17} \,\%\, 466440 = 131072$$
$$\therefore 131072 \text{ is the un-encrypted message Bob was sending to Alice.}$$