MATH 222

Assignment#3

Due: 5pm on the date stated in the course outline.
Hand in to the assignment box on the 3rd floor of CAB.

1. Using the keystream

	11111	00000	11111	00000	11111	00000	11111
decode	11000	00000	10100	00101	01001	00000	00111

Solution:
Add the columns
in mod 2:

	00111	00000	01011	00101	10110	00000	11000
Convert to decimal:	7	0	11	5	22	0	24

Therefore, the plain text is:

HALFWAY

2. Decipher the following message which was encrypted using the seed I.

J S R V J

Solution:

$$\begin{aligned} 9-8 &\equiv 1 \mod 26 \\ 18-1 &\equiv 17 \mod 26 \\ 17-17 &\equiv 0 \mod 26 \\ 21-0 &\equiv 21 \mod 26 \\ 9-21 &\equiv 14 \mod 26 \end{aligned}$$

Therefore, the plain text is:

BRAVO

3. Decipher the following three messages:

   a) Xli wigsrh qiwweki aew irgvctxih ywmrk xli pmriev gshi amxl e xlvii erh o wmb.

   b) Yw lw lbs vwoflb vnwwf wv MGJ, wt lbs jonnslet-jwgfp tsgfsil lbs snsrglwf ei g ismfsl uwfp. Ois el lw psmezbsf lbs lbefp qsiigys.

   c) Jzwck nhf! Bwm jrzx idzfgu jnpo ustbw.

Solution.

(a) Xli wigsrh qiwweki aew irgvctxih ywmrk xli pmriev gshi amxl e xlvii erh o wmb.

This message was encrypted using a generalized Caesar's Code with $E(x) = x + 4 \pmod{26}$. Thus, $D(y) = y + 22 \pmod{26}$. The decrypted message is,

"**The second message was encrypted using the linear code with *a* three and *k* six.**"

(b) Yw lw lbs vwoflb vnwwf wv MGJ, wt lbs jonnslet-jwgfp tsgfsil lbs snsrglwf ei g ismfsl uwfp. Ois el lw psmezbsf lbs lbefp qsiigys.

This message was encrypted using a linear code with $E(x) = 3x + 6 \pmod{26}$. Thus, $D(y) = 9y + 24 \pmod{26}$. The decrypted message is,

"**Go to the fourth floor of CAB, on the bulletin-board nearest the elevator is a secret word. Use it to decipher the third message.**"

(c) Jzwck nhf! Bwm jrzx idzfgu jnpo ustbw.

This message was encrypted using the key phrase "DISCRETE". The decrypted message is,

"**Great job! You have earned full marks.**"

4. The following message was encrypted using a linear code. Decipher the message.

"B ibatn ubag rq lbgwnlbgzhd pwzhw enhrlnd jdnqji knmnirunk pzgw bedrijgniv or kndzan gr en jdnqji, bok zo b dzgjbgzro pwnan orerkv hrjik urddzeiv forp zo pwbg banb zg prjik enhrln jdnqji; bok gwnan pnan or tnonabi zokzhbgzrod gwbg zg nmna prjik en dr."

-Crwo mro Onjlboo

Solution: The letter "N" appears most often; also the letter B appears often and seems to be representing a word with a single letter. We start with a logical assumption:

$$E(E) \equiv N$$

$$E(A) \equiv B$$

Since the cipher text was encoded using a linear code we have:

$$E(4) \equiv a(4) + k \equiv 13 \pmod{26}$$

$$E(0) \equiv a(0) + k \equiv 1 \pmod{26}$$

Therefore $k = 1$ and subtracting the two congruencies gives:

$$4a \equiv 12 \pmod{26}$$

$$\Rightarrow a \equiv 3 \text{ or } 16 \pmod{26}$$

Since 16 is not invertible $a = 3$. The Encoding function is:

$$E(x) \equiv 3x + 1 \pmod{26}$$

and corresponds to the decoding function:

$$D(x) \equiv 9(x - 1) \pmod{26}$$

which decodes the letters so that:

Cipher text	A	B	C	D	E	F	G	H	I	J	K	L	M
Plain text	R	A	J	S	B	K	T	C	L	U	D	M	V

Cipher text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plain text	E	N	W	F	O	X	G	P	Y	H	Q	Z	I

Resulting in the plaintext:

A large part of mathematics which becomes useful developed with absolutely no desire to be useful, and in a situation where nobody could possibly know in what area it would become useful; and there were no general indications that it ever would be so. -John von Neumann

5. Find a closed form for

$$S_3 = 1^3 + 2^3 + 3^3 + \cdots + n^3$$

To find the closed form, use the expansion:

$$(x+1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1$$

by plugging in $x = 1, x = 2, x = 3, \ldots, x = n$.

Solution:

Plug in $x = 1,\ x = 2,\ x = 3,\ \ldots,\ x = n$ to the given polynomial:

$$\begin{array}{rl} & 2^4 = 1^4 + 4\cdot 1^3 + 6\cdot 1^2 + 4\cdot 1 + 1 \\ & 3^4 = 2^4 + 4\cdot 2^3 + 6\cdot 2^2 + 4\cdot 2 + 1 \\ & 4^4 = 3^4 + 4\cdot 3^3 + 6\cdot 3^2 + 4\cdot 3 + 1 \\ & \vdots \\ + & (n+1)^4 = n^4 + 4\cdot n^3 + 6\cdot n^2 + 4\cdot n + 1 \\ \hline & S_4 - 1 + (n+1)^4 = S_4 + 4\cdot S_3 + 6\cdot S_2 + 4\cdot S_1 + n. \end{array}$$

$$\Rightarrow \quad -1 + (n+1)^4 = 4\cdot S_3 + 6\cdot\frac{(2n+1)(n+1)n}{6} + 4\cdot\frac{(n+1)n}{2} + n$$

$$\Rightarrow \quad 4\cdot S_3 = -1 + (n+1)^4 - (2n+1)(n+1)n - 2\,(n+1)n - n$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)^4 - (2n+1)(n+1)n - 2\,(n+1)n - (n+1)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot\left((n+1)^3 - (2n+1)n - 2\,n - 1 \right)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot\left(n^3 + 3\cdot n^2 + 3\cdot n + 1 - 2n^2 - n - 2\,n - 1 \right)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot(n^3 + n^2)$$

$$\Rightarrow \quad S_3 = \left(\frac{(n+1)n}{2}\right)^2$$

6. Find a closed form for

$$a_n = 1^2 \cdot n \ + \ 2^2 \cdot (n-1) \ + \ 3^2 \cdot (n-2) + \cdots + \ n^2 \cdot 1$$

for $n \geq 1$.

Solution:

$$a_n = 1^2 \cdot n \ + \ 2^2 \cdot (n-1) \ + \ 3^2 \cdot (n-2) + \cdots + \ n^2 \cdot 1$$

$$= \sum_{i=1}^{n} i^2 \, (n+1-i)$$

$$= \sum_{i=1}^{n} (n+1)i^2 - i^3$$

$$= (n+1) \sum_{i=1}^{n} i^2 - \sum_{i=1}^{n} i^3$$

$$= (n+1) \frac{n(n+1)(2n+1)}{6} - \left(\frac{(n+1)n}{2} \right)^2$$

$$= n(n+1)^2 \left(\frac{2n+1}{6} - \frac{n}{4} \right)$$

$$= n(n+1)^2 \left(\frac{4n+2}{12} - \frac{3n}{12} \right)$$

$$= \frac{n(n+1)^2(n+2)}{12}$$

7. Let a_n be the number of words (strings) of length n that can be made using the digits $\{0,1,2,3\}$ with an odd number of twos. Find a recurrence relation for a_n and solve the recurrence. The first few values of a_n are calculated for you.

$a_1 = 1$ 2

$a_2 = 6$ 20 21 23 02 12 32

$a_3 = 28$ 200 201 203 210 211 213 230 231 233 222
020 021 023 002 012 032
120 121 123 102 112 132
320 321 323 302 312 332

Solution:

Notice that there are a total of 4^n words of length n using the digits $\{0,1,2,3\}$. It follows that there are $4^n - a_n$ such words of length n with an even number of twos. There are two cases for the first digit in the word: the first digit is either a 2 or not.

If the first digit is not a 2, then it can be a 0, 1, or 3. Thus, there are $3a_{n-1}$ such words of length n with an odd number of twos. Further, if the first digit is a 2, then there are $4^{n-1} - a_{n-1}$ such words of length n with an odd number of twos. Therefore by adding the two cases together we get

$$\begin{aligned} a_n &= 3a_{n-1} + 4^{n-1} - a_{n-1} \\ &= 2a_{n-1} + 4^{n-1} \\ &= 2a_{n-1} + 2^{2n-2} \end{aligned}$$

This gives the recurrence relation:

$$\boxed{\begin{aligned} a_1 &= 1 \\ a_n &= 2a_{n-1} + 2^{2n-2} \end{aligned}}$$

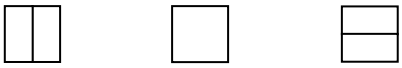
Solve by iteration:

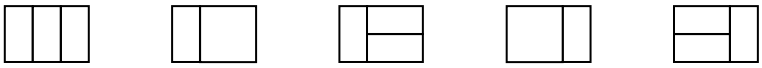
$a_1 = 1 = 2^0$

$$\begin{aligned} a_2 &= 2^1 + 2^2 \\ a_3 &= 2^2 + 2^3 + 2^4 \\ a_4 &= 2^3 + 2^4 + 2^5 + 2^6 \\ &\vdots \\ a_n &= 2^{n-1} + 2^n + \cdots + 2^{2n-2} \\ &= (2^0 + 2^1 + \cdots + 2^{n-2}) + 2^{n-1} + 2^n + \cdots + 2^{2n-2} \\ &\quad -(2^0 + 2^1 + \cdots + 2^{n-2}) \\ &= (2^{2n-1} - 1) - (2^{n-1} - 1) \\ &= 2^{2n-1} - 2^{n-1} \\ &= \boxed{2^{n-1}(2^n - 1)} \end{aligned}$$

8. Let a_n be the number of ways can you tile a $2 \times n$ rectangle using dominoes and square tetrominoes. Dominoes are of size 2×1 and tetrominoes are of size 2×2. Find a recurrence relation for a_n; you do not have to solve this recurrence. The first few values of a_n are calculated for you.

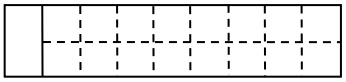
$a_1 = 1$ 

$a_2 = 3$ 

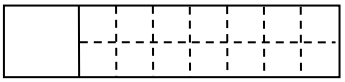
$a_3 = 5$ 

Solution:

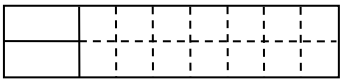
Notice that there are three ways to tile the two most left squares in the $2 \times n$ rectangle:



There are a_{n-1} ways to tile the rest of the rectangle



There are a_{n-2} ways to tile the rest of the rectangle

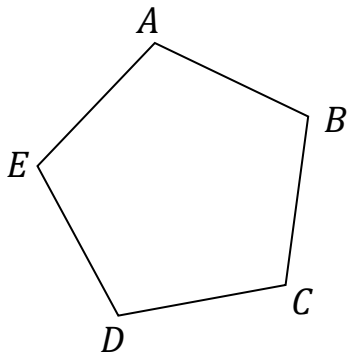


There are a_{n-2} ways to tile the rest of the rectangle

Adding together the cases gives the recurrence relation: $a_n = a_{n-1} + 2a_{n-2}$; $a_1 = 1$, $a_2 = 3$

This is enough for full marks, however you may be interested to know that the solved form for this recurrence relation is $a_n = \frac{1}{3}(-1)^n + \frac{2}{3}2^n$.

9. Let a_n be the number of ways a bug can start at vertex A of the regular pentagon below and reach vertex C for the first time after n moves. A move is made from one vertex to an adjacent vertex. Find a recurrence relation for a_n; you do not have to solve this recurrence. The first four values of a_n are: $a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 2$.



Solution:

Number of Moves	Paths to C (for the first time)	Result
1	None	$a_1 = 0$
2	$A - B - C$	$a_2 = 1$
3	$A - E - D - C$	$a_3 = 1$
4	$A - B - A - B - C$ $A - E - A - B - C$	$a_4 = 2$
5	$A - B - A - E - D - C$ $A - E - A - E - D - C$ $A - E - D - E - D - C$	$a_5 = 3$

Consider the bug's choice for the first move: the bug can either go to E or to B:

- If the bug goes to B, it must return to A (when $n \geq 3$). Therefore, in this case there are a_{n-2} ways the bug can reach vertex C for the first time.
- If the bug goes to E, use the symmetry of the pentagon to conclude there are a_{n-1} ways the bug can reach vertex C for the first time.

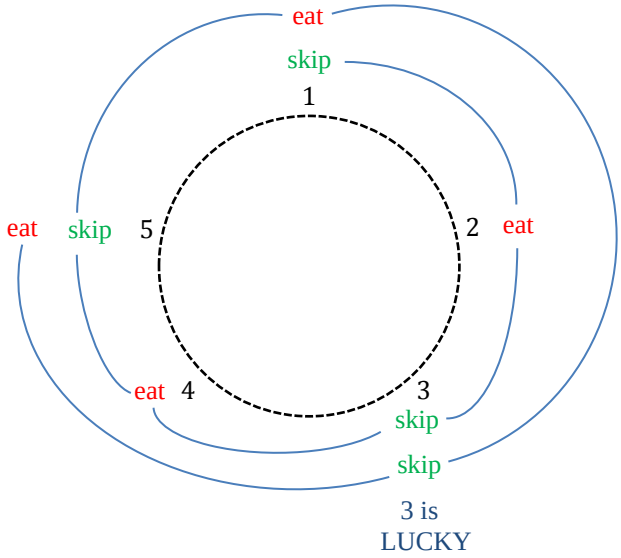
Adding together the two cases gives the recurrence relation:

$$a_1 = 0$$
$$a_2 = 1$$
$$a_n = a_{n-1} + a_{n-2} \qquad n \geq 3$$

10. Sylvester caught n mice which he arranged in a circle and numbered them 1,2, … , n in clockwise order. Starting with mouse number 1, Sylvester went around the circle in clockwise order, skipping over one mouse and eating the next one. He went round and round by the same rule, until only one mouse was left. This lucky mouse was then set free. Denote $f(n)$ as the number assigned to the lucky mouse initially. Now

    $f(1) = 1,\ f(2) = 1, f(3) = 3, f(4) = 1,$ and $f(5) = 3.$

    For example to find $f(5)$:



    (a) Express $f(2n)$ and $f(2n+1)$ in terms of $f(n)$
    (b) Given that $f(530) = 37$, determine $f(2121)$.

Solution:

(a) If there are $2n$ mice, Sylvester will eat all the even-numbered mice in the first round. He is then left with n mice. If the k-th mouse is the lucky one when there are n mice, then the k-th odd-numbered mouse is the lucky one when there are $2n$ mice. The k-th odd-numbered mouse is $2k-1$, and this gives $f(2n) = 2f(n) - 1$. If there are $2n+1$ mice, Sylvester will eat all the even-numbered mice in the first round, with mouse number 1 as desert. He is again left with n mice. Now $(k+1)$-st odd-numbered mouse is the lucky one, and it follows that: $f(2n+1) = 2f(n) + 1$.

(b) $f(2121) = 2f(1060) + 1 = 2(2f(530) - 1) + 1 = 4 \cdot 37 - 2 + 1 = 147$

Bonus.

The Mayor of Edmonton wants Dr. Ecco to help him with plans for the new arena. Dr. Ecco isn't interested so the Mayor sends his goons to bring him in. Dr. Ecco sends out a decoy cipher text to mislead the goons. The cipher text is as follows:

O oy pwknmxg m pyrfc ob ZQNP

Except for the last word, the mayor has found the plain text:

I am hosting a party in

a) Dr. Ecco's decoy cipher text was encoded using the Hill cipher with the encoding function:

$$E(x) \equiv 5 \cdot x + 6 \cdot y \pmod{26}$$
$$E(y) \equiv 18 \cdot x + y \pmod{26}$$

Complete the decoy message by finding the decoding function and decode the last word of the cipher text. If the mayor's goons follow Dr. Ecco's decoy message where will they end up going?

b) Dr. Ecco has double-encoded the last word in his message. To get the real message, you must suppose that the plain text word found in part a) is also cipher text. What is the real message?

Solution:

Start by finding the decoding function:

$$\begin{bmatrix} 5 & 6 \\ 18 & 1 \end{bmatrix}^{-1} \equiv (5 \cdot 1 - 6 \cdot 18)^{-1} \begin{bmatrix} 1 & -6 \\ -18 & 5 \end{bmatrix} \equiv \begin{bmatrix} 1 & -6 \\ 8 & 5 \end{bmatrix} \pmod{26}$$

Therefore,

$$\begin{aligned} D(x) &\equiv x - 6 \cdot y \pmod{26} \\ D(y) &\equiv 8 \cdot x + 5 \cdot y \pmod{26} \end{aligned}$$

a)

$$\begin{aligned} D(Z) &\equiv (-1) - 6 \cdot (-10) \equiv 7 \pmod{26} \\ D(Q) &\equiv 8 \cdot (-1) + 5 \cdot (-10) \equiv 20 \pmod{26} \end{aligned}$$

$$\begin{aligned} D(N) &\equiv (13) - 6 \cdot (15) \equiv 1 \pmod{26} \\ D(P) &\equiv 8 \cdot (13) + 5 \cdot (15) \equiv -3 \pmod{26} \end{aligned}$$

The decoy message is: HUB

$$\begin{aligned} D(H) &\equiv (7) - 6 \cdot (20) \equiv 17 \pmod{26} \\ D(U) &\equiv 8 \cdot (7) + 5 \cdot (20) \equiv 0 \pmod{26} \end{aligned}$$

$$\begin{aligned} D(B) &\equiv (1) - 6 \cdot (-3) \equiv 19 \pmod{26} \\ D(X) &\equiv 8 \cdot (1) + 5 \cdot (-3) \equiv 19 \pmod{26} \end{aligned}$$

The real message is: RATT