Chapter 17
Information Science

For All Practical Purposes: Effective Teaching

- When administering an exam, try to arrive a little early to class. If you spot an error on the exam while it is being administered, make a judgment regarding its overall impact on the exam. If you feel that it is something that will cause students to spend valuable time, then it may be best to announce the correction or question deletion to the class. Be mindful though about how students are progressing and if any students turned in a completed exam not knowing there was an unintended error.
- When students take exams, they may expect extra time at the end to complete their work. When the exam is administered, be clear as to how much time they have to work on it. The main issue is fairness to all students. Some students may have scheduled back-to-back classes and would be disadvantaged by not imposing a limited examination time for all students.

Chapter Briefing

In this chapter we consider some sophisticated techniques to detect and correct errors in digitally transmitted messages. We also take a look at methods that have been developed for the compression of data and for protection of the confidentiality of our messages. The Internet was originally used only by a few organizations as a source of information, but use of the Internet has become far more widespread. Now the Internet is used for shopping, entertainment, games, and much more. Web search efficiency is of importance with such wide spread use.

Being well prepared for class discussion with examples is essential. In order to facilitate your preparation, the **Chapter Topics to the Point** has been broken down into **Binary Codes and Check Digits**, **Data Compression**, **Modular Arithmetic**, **Encryption**, and **Mathematical Logic**. Examples with solutions for these topics that do not appear in the text nor study guide are included in the *Teaching Guide*. You should feel free to use these examples in class, if needed.

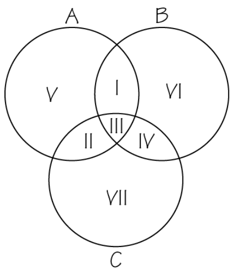
Since you may demonstrate some techniques of this chapter using a calculator, the *Teaching Guide* includes the feature **Teaching the Calculator**. It includes brief calculator instructions with screen shots from a TI-83.

The last section of this chapter of *The Teaching Guide for the First-Time Instructor* is **Solutions to Student Study Guide ✎ Questions**. These are the complete solutions to the five questions included in the *Student Study Guide*. Students only have the answers to these questions, not the solutions.

Chapter Topics to the Point

Binary Codes and Check Digits

Most computerized data are stored and transmitted as sequences of 0's and 1's. We can store a data string of length 4 in regions I through IV, respectively. Regions V, VI, and VII have appended digits so that the sum of the regions for each circle has **even parity**. The encoded messages are called **code words**. This scheme is helpful to detect and even correct errors.

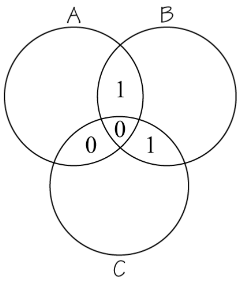


Example

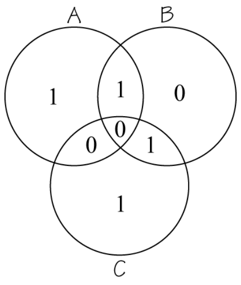
Store the data string 1001 along with its appended digits correctly in a three-circle diagram. What is the code word?

Solution

Original data string



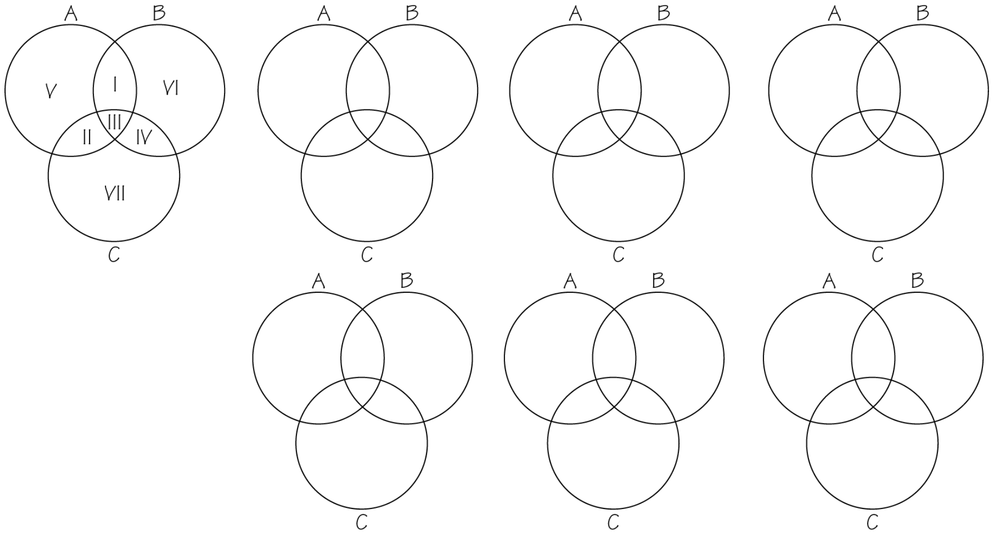
Coded data string



The code word is 1001101.

Teaching Tip

You may choose to make a handout with the following to assist in this component of the lecture. A difficult part is remembering the labeling of the regions.



If a string of digits $a_1\ a_2\ a_3\ a_4$ is a message, then we can create a code word in a **binary linear code** by adding check digits that are the **parity-check sums** $a_1 + a_2 + a_3$, $a_1 + a_3 + a_4$, and $a_2 + a_3 + a_4$. If the sum is even, a check digit of 0 is appended. If it is odd, then a 1 is appended. Other rules for adding digits are possible.

Since there may be errors in the coding process or transmission, we use the **nearest-neighbor decoding method** to find the code word with the shortest distance (number of positions in which the strings differ) from the received message. Use Table 17.1 on page 620.

The weight of a binary code is the minimum number of 1's that occur among all nonzero code words of that code.

Example

What is the code word for the message 11001? Append two check digits using the parity-check sums $a_1 + 2a_2 + a_3$ and $3a_1 + a_3 + a_5$.

Solution

$a_1 + 2a_2 + a_3 = 3$, odd parity; so the first check digit is 1. $3a_1 + a_3 + a_5 = 4$, even parity; so the last check digit are 0. The code word is therefore, 1100110.

⮳ Data Compression

In encoding a sequence of letters with a binary code (or decoding the binary code), we need an assignment of letters and code.

Example

Use $A \to 0,\ B \to 10,\ C \to 110,\ D \to 1110,\ E \to 11110,$ to decode the following.

011011011110110111000

Solution

Noticing the location of the zeros, 011011011110110111000 can be written as 0, 110, 110, 11110, 110, 1110, 0, 0. Thus we have, *ACCECDAA*.

Huffman coding assigns to letters of the alphabet strings of variable size depending on the frequency a letter occurs or an assigned probability. To do this one needs to create a code tree (binary tree) performing the following steps.

- List the letters in increasing order top to bottom in terms of their probabilities. Note: The sum of the probabilities will be 1.
- The two letters that have the lowest probability of occurring get grouped together. Their probabilities are summed and the letter that has the smallest probability of occurring appears on the left. Rearrange the letters (two are grouped together), if necessary, in terms of their probabilities of occurring. From here on out a group of letters can consist of more than one letter.
- Continue this process with the new list until all letters appear in a string and the probability is 1.
- The letters/combination of letters are now spread out into a tree, working backwards. Figure 17.7 on page 633 demonstrates this with *EC* having probability 0.425 placed with a 0 on the top branch and *FDBA* having probability 0.575 placed with a 1 on the bottom branch.
- Read the variable string code for the letters right to left.

☝Teaching Tip

You may choose to investigate Websites to create code such as the following.

http://www.cs.ttu.edu/~eacosta/java/Huffcode/Huffcode.html.

Example

Use a Huffman tree code to assign a binary code given the following.

A	*B*	*C*	*D*
0.12	0.60	0.10	0.18

Solution

Arranging these in order, we have the following.

C	0.10
A	0.12
D	0.18
B	0.60

Since *C* and *A* are the least likely to occur, we begin the tree by merging them.

CA	0.22
D	0.18
B	0.60

Rearranging we have the following.

D	0.18
CA	0.22
B	0.60

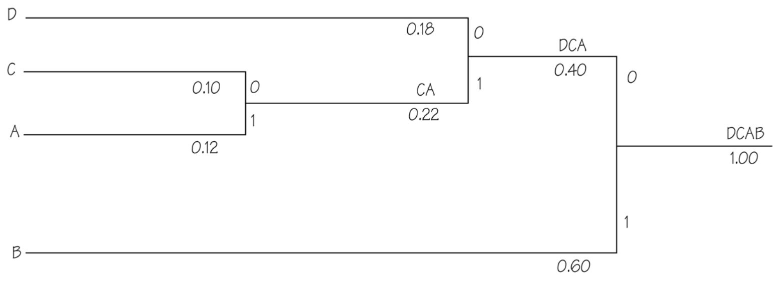
Now *D* and *CA* are least likely, so we merge them.

DCA	0.40
B	0.60

And finally,

DCAB	1.00

Working backwards we have the following diagram. Read the diagram from right to left.



The Huffman tree code assigns a binary code as follows.

A = 011, *B* = 1, *C* = 010, *D* = 00

Note that these assignments have variable lengths.

Modular Arithmetic

The notation $a \bmod n$ is read as ***a* modulo *n***. *a* and *n* are both positive integers. $a \bmod n$ is the remainder when *a* is divided by *n*. The multiplication property for modular arithmetic, which is $(ab) \bmod n = \big((a \bmod n)(b \bmod n)\big) \bmod n,$ allows for simpler calculations which can be performed in a variety of ways.

Example

Simplify $(11^7 \cdot 13) \bmod 7.$

Solution

$$(11^7 \cdot 13) \bmod 7 = \left[(11^2 \bmod 7)^3 (11 \bmod 7)(13 \bmod 7)\right] \bmod 7 = \left[(121 \bmod 7)^3 (11 \bmod 7)(13 \bmod 7)\right] \bmod 7$$

$$(121 = 17 \cdot 7 + 2)$$

$$= \left[(2 \bmod 7)^3 (4)(6)\right] \bmod 7 = \left[(8)(24)\right] \bmod 7$$

$$= \left[(8 \bmod 7)(24 \bmod 7)\right] \bmod 7 = \left[(1)(3)\right] \bmod 7 = 3 \bmod 7 = 3$$

Encryption

The so-called **Caesar cipher** is a cryptosystem that assigns a letter of the alphabet to another letter of the alphabet by shifting each letter of the alphabet by a fixed algorithm. Since there is a limited number of letters of the alphabet, there is a limited number of possible shifts.

The **Vigenère cipher** requires a key word that will first shift each letter of the word to be encoded. Each letter of the word to be encoded is identified by a position 0 – 25 (A is located in position 0, not 1). The code word then shifts each letter, and that result is evaluated modulo 26.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Location	0	1	2	3	4	5	6	7	8	9	10	11	12

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Location	13	14	15	16	17	18	19	20	21	22	23	24	25

Example

Use the Vigenère cipher with the keyword HI to encrypt the message PIZZA.

Solution

H is in the position 7 and I is in position 8.

Original	Location			Encrypted
P	15	7	$(15+7) \bmod 26 = 22 \bmod 26 = 22$	W
I	8	8	$(8+8) \bmod 26 = 16 \bmod 26 = 16$	Q
Z	25	7	$(25+7) \bmod 26 = 32 \bmod 26 = 6$	G
Z	25	8	$(25+8) \bmod 26 = 33 \bmod 26 = 7$	H
A	0	7	$(0+7) \bmod 26 = 7 \bmod 26 = 7$	H

The encrypted message would be WQGHH.

Question

Given that PI was used as a key word for the Vigenère cipher to encrypt RQGKAM, what is the decrypted message?

Solution

Encrypted	Location				Decrypted
R	17	15	$17 = 17 \bmod 26 = (2+15) \bmod 26$	2	C
Q	16	8	$16 = 16 \bmod 26 = (8+8) \bmod 26$	8	I
G	6	15	$6 = 32 \bmod 26 = (17+15) \bmod 26$	17	R
K	10	8	$10 = 10 \bmod 26 = (2+8) \bmod 26$	2	C
A	0	15	$0 = 26 \bmod 26 = (11+15) \bmod 26$	11	L
M	12	8	$12 = 12 \bmod 26 = (4+8) \bmod 26$	4	E

The original message was CIRCLE.

Teaching Tip

Relay to students that decrypting a message is more involved than encrypting a message using the Vigenère cipher. They should be comfortable going in both directionswith both encrytion and decryption.

☝Teaching Tip

If you are wanting to avoid modular arithmetic, then the following table can be used to encode and decode using the Vigenère cipher as well as the Caesar cipher. For the Caesar cipher, the first row is a shift of 0; the second is a shift of 1; and the last is a shift of 25. You may choose to photocopy this table.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Another type of encryption is a **Cryptogram** one letter stands for another. By examining the frequency that a letter occurs, one can try to decipher it.

☝Teaching Tip

In the method of matching strings by "addition": 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0. Two strings match if they "add" to a string of 0's. Students may confuse this form of "addition" with adding in base-2.

RSA public key encryption involves a procedure involving prime numbers and modular arithmetic. The procedure for sending and receiving messages is outlined on pages 642 – 643 of the text. In this form of encryption, letters start with 01 and a space is 00.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Location	01	02	03	04	05	08	07	08	09	10	11	12	13

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Location	14	15	16	17	18	19	20	21	22	23	24	25	26

Example

Use the RSA scheme with $p = 13,\ q = 11,$ and $r = 7$ to decode the received numbers 82, 115, 6. (It may have been sent as 082115006.)

Solution

1. Since $p = 13,\ q = 11,\ \ n = pq = 13 \cdot 11 = 143.$
2. Since $p - 1 = 13 - 1 = 12$ and $q - 1 = 11 - 1 = 10,$ m will be the least common multiple of 12 and 10, namely 60.
3. We need to choose r such that it has no common divisors with 60. Thus, r can be 7. This confirms that $r = 7$ is a valid choice.
4. We need to find s.

$$r^2 \bmod m = 7^2 \bmod 60 = 49 \bmod 60 = 49$$

$$r^3 \bmod m = 7^3 \bmod 60 = 343 \bmod 60 = (5 \cdot 60 + 43) \bmod 60 = 43$$

$$r^4 \bmod m = 7^4 \bmod 60 = 2401 \bmod 60 = (40 \cdot 60 + 1) \bmod 60 = 1$$

Thus $t = 4.$

Since $s = r^{t-1} \bmod m,$ where $r = 7$, $m = 60,$ and $t = 4,$ we have the following.

$$s = 7^{4-1} \bmod 60 = 7^3 \bmod 60 = 43$$

5. Since $82^{43} \bmod 143 = \left[\left(82^4\right)^{10} \cdot 82^3\right] \bmod 143$

$$\begin{aligned}
&= \left[\left(\left(82^4\right) \bmod 143\right)^{10} \cdot \left(82^3 \bmod 143\right)\right] \bmod 143 \\
&= \left[\left(45212176 \bmod 143\right)^{10} \cdot \left(551368 \bmod 143\right)\right] \bmod 143 \\
&= \left(9^{10} \cdot 103\right) \bmod 143 \\
&= \left[\left(9^{10} \bmod 143\right) \cdot 103\right] \bmod 143 \\
&= \left[\left(3486784401 \bmod 143\right) \cdot 103\right] \bmod 143 \\
&= \left(100 \cdot 103\right) \bmod 143 = 10300 \bmod 143 = 4,\ \ R_1 = 4.
\end{aligned}$$

Continued on next page

$$
\begin{aligned}
\text{Since } 115^{43} \bmod 143 &= \left[\left(115^{4}\right)^{10} \cdot 115^{3}\right] \bmod 143 \\
&= \left[\left(\left(115^{4}\right) \bmod 143\right)^{10} \cdot \left(115^{3} \bmod 143\right)\right] \bmod 143 \\
&= \left[\left(174900625 \bmod 143\right)^{10} \cdot \left(1520875 \bmod 143\right)\right] \bmod 143 \\
&= \left(42^{10} \cdot 70\right) \bmod 143 \\
&= \left[\left(42^{5}\right)^{2} \cdot 70\right] \bmod 143 \\
&= \left[\left(\left(42^{5}\right) \bmod 143\right)^{2} \cdot 70\right] \bmod 143 \\
&= \left[\left(130691232 \bmod 143\right)^{2} \cdot 70\right] \bmod 143 \\
&= \left(100^{2} \cdot 70\right) \bmod 143 = 700000 \bmod 143 = 15,\ R_2 = 15.
\end{aligned}
$$

$$
\begin{aligned}
\text{Since } 6^{43} \bmod 143 &= \left[\left(2^{20}\right)^{2} \cdot 2^{3} \cdot \left(3^{20}\right)^{2} \cdot 3^{3}\right] \bmod 143 \\
&= \left[\left(\left(2^{20}\right) \bmod 143\right)^{2} \cdot 2^{3} \cdot \left(\left(3^{20}\right) \bmod 143\right)^{2} \cdot 3^{3}\right] \bmod 143 \\
&= \left(100^{2} \cdot 100^{2} \cdot 216\right) \bmod 143 \\
&= \left(\left(100^{2} \bmod 143\right)^{2} \left(216 \bmod 143\right)\right) \bmod 143 \\
&= \left(133^{2} \cdot 73\right) \bmod 143 = 1291297 \bmod 143 = 7,\ R_3 = 7.
\end{aligned}
$$

Thus, the message is DOG.

Mathematical Logic

An expression in **Boolean logic** is simply a statement that is either true or false. Many search engines allow users to construct searches using Boolean logic.

A **truth table** lists the values for an expression for all possible combinations of the Boolean variables *P* and *Q*. The letter T is used to indicate that an expression is true, and the letter F indicates that an expression is false.

The **connectives** AND, OR, and NOT can be used to construct complex Boolean expressions.

- The expression NOT *P* is called the **negation** of *P*. If *P* is true then NOT *P* is false, and if *P* is false then NOT *P* is true. The standard mathematical notation for this is $\neg P$.
- The truth table is as follows.

P	$\neg P$
T	F
F	T

- The expression *P* AND *Q* is called the **conjunction** of *P* and *Q*. This expression is true when both *P* and *Q* are true and is false otherwise. The standard mathematical notation for this is $P \wedge Q$.
- The truth table is as follows.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

- The expression *P* OR *Q* is called the **disjunction** of *P* and *Q*. This expression is true if either *P* or *Q* (or both) are true and is false otherwise. The standard mathematical notation for this is $P \vee Q$.

- The truth table is as follows.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

If two expressions have the same value (true or false) for each possible assignment of the Boolean variables, they are said to be **logically equivalent**.

Example

Is the expression $\neg P \wedge (Q \vee R)$ logically equivalent to $\neg Q \wedge (P \vee R)$?

Solution

First we construct the truth table for $\neg P \wedge (Q \vee R)$.

P	Q	R	$\neg P$	$Q \vee R$	$\neg P \wedge (Q \vee R)$
T	T	T	F	T	F
T	T	F	F	T	F
T	F	T	F	T	F
T	F	F	F	F	F
F	T	T	T	T	T
F	T	F	T	T	T
F	F	T	T	T	T
F	F	F	T	F	F

Next we construct the truth table for $\neg Q \wedge (P \vee R)$.

P	Q	R	$\neg Q$	$P \vee R$	$\neg Q \wedge (P \vee R)$
T	T	T	F	T	F
T	T	F	F	T	F
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	F	T	F	F

Since the last columns of the two truth tables are not identical, the expression $\neg P \wedge (Q \vee R)$ is not logically equivalent to $\neg Q \wedge (P \vee R)$.

☝Teaching Tip

Ask students about what the truth table would look like if there were 4 or 5 statements. See if they notice the pattern that there will be 2^n possible truth value choices for all the statements. Also the first statement (column) starts with $\frac{2^n}{2}$ T's followed by $\frac{2^n}{2}$ F's. See if they can justify why the last column is always made up of alternating T's and F's and why the last row contains only F's.

Teaching the Calculator

The calculator can be very helpful in determining $a \bmod n$. If a is very large (7^{51}, for example), the multiplication property for modular arithmetic should be used. Once a reasonable value for $a \bmod n$ needs to be determined, then we are needing to find the whole numbers q and r such that $a = nq + r$. r will be the value of $a \bmod n$.

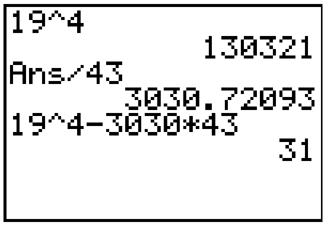
Example

Find the value of $19^{11} \bmod 43$.

Solution

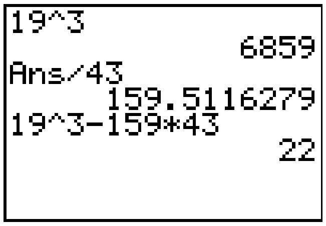
For example $19^{11} \bmod 43 = \left[\left(19^4\right)^2 \cdot 19^3\right] \bmod 43 = \left[\left(19^4 \bmod 43\right)^2 \cdot 19^3 \bmod 43\right] \bmod 43$

$$19^4 \bmod 43 = 31$$



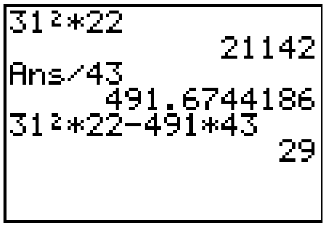
```
19^4
             130321
Ans/43
         3030.72093
19^4-3030*43
                 31
```

$$19^3 \bmod 43 = 22$$



```
19^3
               6859
Ans/43
        159.5116279
19^3-159*43
                 22
```

$$19^{11} \bmod 43 = \left(31^2 \cdot 22\right) \bmod 43 = 21142 \bmod 43 = 29$$



```
31²*22
              21142
Ans/43
        491.6744186
31²*22-491*43
                 29
```

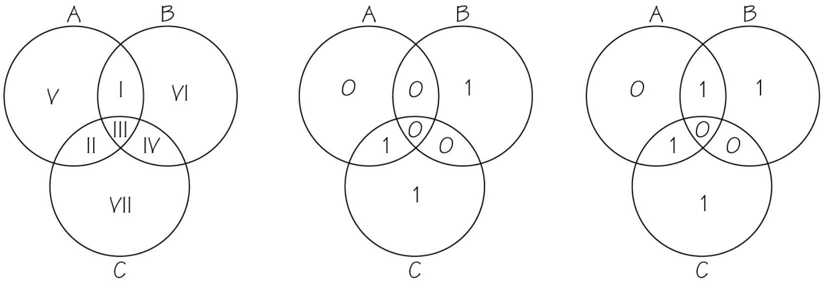
$19^{11} \bmod 43 = 29$.

Solutions to Student Study Guide ✏ Questions

Question 1

If a code word was received as 0100011, what region (if any) would be changed to decode the message using the diagram method?

Solution



In order to have an even parity in all three circles, Region I would be changed.

Question 2

Use a Huffman tree code to assign a binary code given the following.

A	*B*	*C*	*D*	*E*	*F*	*G*
0.105	0.235	0.100	0.115	0.195	0.107	0.143

Solution

Arranging these in order, we have the following.

C	0.100
A	0.105
F	0.107
D	0.115
G	0.143
E	0.195
B	0.235

Since *C* and *A* are the least likely to occur, we begin the tree by merging them.

CA	0.205
F	0.107
D	0.115
G	0.143
E	0.195
B	0.235

Rearranging we have the following.

F	0.107
D	0.115
G	0.143
E	0.195
CA	0.205
B	0.235

Now *F* and *D* are least likely, so we merge them.

FD	0.222
G	0.143
E	0.195
CA	0.205
B	0.235

Rearranging we have the following.

G	0.143
E	0.195
CA	0.205
FD	0.222
B	0.235

Now *G* and *E* are least likely, so we merge them.

GE	0.338
CA	0.205
FD	0.222
B	0.235

Continued on next page

Rearranging we have the following.

CA	0.205
FD	0.222
B	0.235
GE	0.338

Now *CA* and *FD* are least likely, so we merge them.

CAFD	0.427
B	0.235
GE	0.338

Rearranging we have the following.

B	0.235
GE	0.338
CAFD	0.427

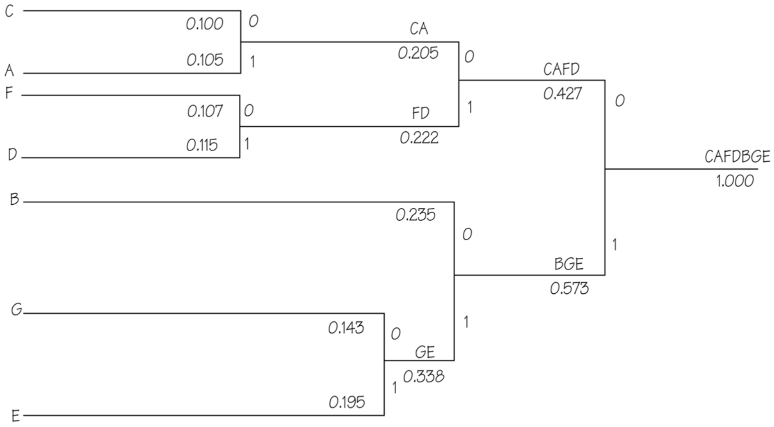
Now *B* and *GE* are least likely, so we merge them.

BGE	0.573
CAFD	0.427

And finally,

CAFDBGE	1.000

Working backwards we have the following diagram.



The Huffman tree code assigns a binary code as follows.

A = 001, *B* = 10, *C* = 000, *D* = 011, *E* = 111, *F* = 010, *G* = 110

Question 3

Given that CUTE was used as a key word for the Vigenère cipher to encrypt OUML KM CSA, what is the decrypted message?

Solution

Encrypted	Location				Decrypted
O	14	2	$14 = 14 \bmod 26 = (12 + 2) \bmod 26$	12	M
U	20	20	$20 = 20 \bmod 26 = (0 + 20) \bmod 26$	0	A
M	12	19	$12 = 38 \bmod 26 = (19 + 19) \bmod 26$	19	T
L	11	4	$11 = 11 \bmod 26 = (7 + 4) \bmod 26$	7	H
K	10	2	$10 = 10 \bmod 26 = (8 + 2) \bmod 26$	8	I
M	12	20	$12 = 38 \bmod 26 = (18 + 20) \bmod 26$	18	S
C	2	19	$2 = 28 \bmod 26 = (9 + 19) \bmod 26$	9	J
S	18	4	$18 = 18 \bmod 26 = (14 + 4) \bmod 26$	14	O
A	0	2	$0 = 26 \bmod 26 = (24 + 2) \bmod 26$	24	Y

The original message was Math is joy.

Question 4

Use the RSA scheme with $p = 13$, $q = 11$, and $r = 7$ to encrypt the message DOG.

Solution

1. DOG converts to 041507.
2. We will send 04, 15, and 07 individually.
3. Since $p = 13$ and $q = 11$, $n = pq = 11 \cdot 13 = 143$.

   Since $\text{GCF}(4,143) = 1$, $\text{GCF}(15,143) = 1$, and $\text{GCF}(7,143) = 1$, we can proceed. Thus, $M_1 = 4$, $M_2 = 15$, and $M_3 = 7$.
4. Since $R_i = M_i^{\,r} \bmod n$ and $r = 7$, we have the following.

   $R_1 = 4^7 \bmod 143 = 16384 \bmod 143 = 82$

   $R_2 = 15^7 \bmod 143 = (3 \cdot 5)^7 \bmod 143 = (3^7 \cdot 5^7) \bmod 143 = \left[(3^7 \bmod 143)(5^7 \bmod 143)\right] \bmod 143$

   $= \left[(2187 \bmod 143)(78125 \bmod 143)\right] \bmod 143 = (42 \cdot 47) \bmod 143 = 1974 \bmod 143 = 115$

   $R_3 = 7^7 \bmod 143 = 823543 \bmod 143 = 6$

Thus, the numbers sent are 82, 115, 6.

Question 5

Is the expression $P \wedge (\neg Q \vee \neg R)$ logically equivalent to $(P \wedge \neg Q) \vee (P \wedge \neg R)$?

Solution

A truth table for $P \wedge (\neg Q \vee \neg R)$ is as follows.

P	Q	R	$\neg Q$	$\neg R$	$\neg Q \vee \neg R$	$P \wedge (\neg Q \vee \neg R)$
T	T	T	F	F	F	F
T	T	F	F	T	T	T
T	F	T	T	F	T	T
T	F	F	T	T	T	T
F	T	T	F	F	F	F
F	T	F	F	T	T	F
F	F	T	T	F	T	F
F	F	F	T	T	T	F

A truth table for $(P \wedge \neg Q) \vee (P \wedge \neg R)$ is as follows.

P	Q	R	$\neg Q$	$P \wedge \neg Q$	$\neg R$	$P \wedge \neg R$	$(P \wedge \neg Q) \vee (P \wedge \neg R)$
T	T	T	F	F	F	F	F
T	T	F	F	F	T	T	T
T	F	T	T	T	F	F	T
T	F	F	T	T	T	T	T
F	T	T	F	F	F	F	F
F	T	F	F	F	T	F	F
F	F	T	T	F	F	F	F
F	F	F	T	F	T	F	F

Because the last columns of these truth tables are identical, we conclude that the two expressions are logically equivalent.