FAST- National University of Computer and Emerging Sciences, Karachi.

FAST School of Computing, Fall 2022

CS1005-Discrete Structures

Assignment # 3 -- Solution

Instructions: **Max. Points: 100**

1- This is hand written assignment.
2- Just write the question number instead of writing the whole question.
3- You can only use A4 size paper for solving the assignment.

---

1. What are the quotient and remainder when:

a) 19 is divided by 7?	Solution:	q = 2;	r = 5
b) −111 is divided by 11?	Solution:	q = -11;	r = 10
c) 789 is divided by 23?	Solution:	q = 34;	r = 7
d) 1001 is divided by 13?	Solution:	q = 77;	r = 0
e) 10 is divided by 19?	Solution:	q = 0;	r = 10
f) 3 is divided by 5?	Solution:	q = 0;	r = 5
g) −1 is divided by 3?	Solution:	q = -1;	r = 2
h) 4 is divided by 1?	Solution:	q = 4;	r = 0

2. (a) Find a div m and a mod m when

	q = *a* div *m*		*r* = *a* mod *m*
i) a = −111, m = 99.	Solution: −2 = −111 div 99	;	87 = −111 div 99
ii) a = −9999, m = 101.	Solution: −99 = −9999 div 101	;	0 = −9999 div 101
iii) a = 10299, m = 999.	Solution: 10 = 10299 div 999	;	309 = 10299 div 999
iv) a = 123456, m = 1001.	Solution: 123= 123456 div 1001	;	333 = 123456 div 1001

(b) Decide whether each of these integers is congruent to 5 modulo 17.

i) 80
Solution:
As We know that $a \equiv b(mod\, m)$ iff $\frac{a-b}{m}$.
Now $80 \not\equiv 5\ (mod\, 17)$ because $\frac{80-5}{17} = 4.41.$
ii) 103
As We know that $a \equiv b(mod\, m)$ iff $\frac{a-b}{m}$.
Now $103 \not\equiv 5\ (mod\, 17)$ because $\frac{103-5}{17} = 5.76.$
iii) −29
As We know that $a \equiv b(mod\, m)$ iff $\frac{a-b}{m}$.
Now $-29 \equiv 5\ (mod\, 17)$ because $\frac{-29-5}{17} = \ -2.$
iv) −122
As We know that $a \equiv b(mod\, m)$ iff $\frac{a-b}{m}$.
Now $-122 \not\equiv 5\ (mod\, 17)$ because $\frac{-122-5}{17} = \ -7.47.$

3. (a) Determine whether the integers in each of these sets are pairwise relatively prime.
i) 11, 15, 19
Solution: Yes
gcd (11,15) = 1,   gcd (11,15) = 1, gcd (11,19) = 1

ii) 14, 15, 21
Solution: No
gcd (14, 15) = 1, gcd (14, 21) = 7, gcd (15, 21) = 3

iii) 12, 17, 31, 37
Solution: Yes
gcd (12, 17) = 1, gcd (12, 31) = 1, gcd (12, 37) = 1, gcd (17, 31) = 1, gcd (17, 37) = 1, gcd (31, 37) = 1

iv) 7, 8, 9, 11
Solution: Yes
gcd (7, 8) = 1, gcd (7, 9) = 1, gcd (7, 11) = 1, gcd (8, 9) = 1, gcd (8, 11) = 1, gcd (9, 11) = 1

(b) Find the prime factorization of each of these integers.

i) 88	Solution: $88 = 2^3 * 11$
ii) 126	Solution: $126 = 2 * 3^2 * 7$
iii) 729	Solution: $729 = 3^6$
iv) 1001	Solution: 1001 = 7 * 13 * 11
v) 1111	Solution: 1111 = 11 * 101
vi) 909	Solution: $909 = 3^2 * 101$

4. Use the extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 100001) as a linear combination.
Solution:
Gcd(144,89) = (144)(34) + (89)(−55) = 1
Gcd (1001, 100001) = (10)(100001) + (−999)(1001) = 11

5. Solve each of these congruences using the modular inverses.
a) 55x ≡ 34 (mod 89)
Solution:
Gcd(55,89) = (55)(34) + (89)(−21) = 1
So, inverse ā = 34.
Multiply 34 both side
55 * 34 x ≡ 34 * 34 (mod 89)
x = 1156 (mod 89) = 88.

b) 89x ≡ 2 (mod 232)
Solution:
Gcd(89,232) = (73)(89) + (232)(−28) = 1
So, inverse ā = 73,
Multiply 73 both side
89 * 73 x ≡ 2 * 73 (mod 232)
x = 146 (mod 232) = 146.

6. (a) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences.

i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

We have $m=m_1 * m_2 * m_3 = 5 * 6 * 7 = 210$.

$M_1= 210/5 = 42$, $M_2 = 210/6 = 35$, and $M_3 = 210/7 = 30$

Also, by simple inspection we see that:

$y_1 = 3$ is an inverse for $M_1 = 42$ modulo 5, $y_2 = 5$ is an inverse for $M_2 = 35$ modulo 6 and

$y_3 = 4$ is an inverse for $M_3 = 30$ modulo 7.

The solutions to the system are then all numbers x such that

$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3) \bmod m = ((1 * 42 * 3) + (2*35*5) + (3*30*4)) \bmod 210$

$= 836 \pmod{210} = 206$.

ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

We have $m=m_1 * m_2 * m_3 * m_4 = 2 * 3 * 5 * 11 = 330$.

$M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$ and $M_4= 330/11 = 30$

Also, by simple inspection we see that:

$y_1 = 1$ is an inverse for $M_1= 165$ modulo 2, $y_2 = 2$ is an inverse for $M_2 = 110$ modulo 3,

$y_3= 1$ is an inverse for $M_3 = 66$ modulo 5 and $y_4 = 7$ is an inverse for $M_4 = 30$ modulo 11.

The solutions to the system are then all numbers x such that

$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4) \bmod m$

$= ((1 * 165 * 1) + (2 * 110 *2) + (3 * 66 *1) + (4 * 30 *7)) \bmod 330 = 1643 \pmod{330} = 323$.

(b) An old man goes to market and a camel step on his basket and crushes the oranges. The camel rider offers to pay for the damages and asks him how many oranges he had brought. He does not remember the exact number, but when he had taken them out five at a time, there were 3 oranges left. When he took them six at a time, there were also three oranges left, when he had taken them out seven at a time, there was only one orange was left and when he had taken them out eleven at a time, there was no orange left. What is the number of oranges he could have had?

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

We have $m=m_1 * m_2 * m_3 * m_4 = 2310$.

Also, by simple inspection we see that:

$y_1 = 3$ is an inverse for $M_1 = 462$ modulo5, $y_2 = 1$ is an inverse for $M_2 = 385$ modulo 6,

$y_3 = 1$ is an inverse for $M_3 = 330$ modulo 7 and $Y_4 = 1$ is an inverse for $M_3 = 210$ modulo 11.

The solutions to the system are then all numbers x such that

$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4) \bmod m$

$= (3 * 462 * 3) + (3* 385* 1) + (1* 330* 1) + (0*210*1) = 5643 \pmod{2310} = 1023$.

He could have 1023 oranges.

7. Find an inverse of a modulo m for each of these pairs of relatively prime integers.

a) $a = 2$, $m = 17$

Solution:

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

So, $-8 + 17 = 9$ Hence inverse, $\bar{a} = 9$.

b) a = 34, m = 89
Solution:
gcd(34,89) = (13)(89) + (−34)(34) = 1
So, −34 + 89 = 55 Hence inverse, $\bar{a}$ = 55.

c) a = 144, m = 233
Solution:
gcd(144,233) = (89)(144) + (−55)(233) = 1 Hence inverse, $\bar{a}$ = 89.

d) a = 200, m = 1001
Solution:
gcd(200,1001) = (1)(1001) + (−5)(200) = 1
So, −5 + 1001 = 996 Hence inverse, $\bar{a}$ = 996.

8. (a) Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
i) f (p) = (p + 4) mod 26
Solution:
S T O P P O L L U T I O N
18 19 14 15 15 14 11 11 20 19 8 14 13
After applying function:
22 23 18 19 19 18 15 15 24 23 12 18 17
W X S T T S P P Y X M S R will be encrypted message.

ii) f (p) = (p + 21) mod 26
Solution:
S T O P P O L L U T I O N
18 19 14 15 15 14 11 11 20 19 8 14 13
After applying function:
13 14 09 10 10 09 06 06 15 14 03 09 08
N O J K K J G G P O D J I will be encrypted message.

(b) Decrypt these messages encrypted using the Shift cipher. f (p) = (p + 10) mod 26.
i) CEBBOXNOB XYG
Solution:
"SURRENDER NOW" will be decrypted message.

ii) LO WI PBSOXN
Solution:
"BE MY FRIEND" will be decrypted message.

9. Use Fermat's little theorem to compute 5^{2003} mod 7, 5^{2003} mod 11, and 5^{2003} mod 13.
Solution:
(i) 5^{2003} mod 7
Solution: Since $5^6 = 1$ mod 7
$= (5^6)^{333} . 5^5$ mod 7 $= 5^5$ mod 7 = 3.

(ii) 5^{2003} mod 11

Solution: **Since 5^{10} = 1 mod 11**

= $(5^{10})^{2000} . 5^3$ mod 11 = 5^3 mod 11 = 4.

(iii) 5^{2003} mod 13

Solution: **Since 5^{12} = 1 mod 13**

= $(5^{12})^{166} . 5^{11}$ mod 13 = 5^{11} mod 13 = 8.

10. (a) Encrypt the message I LOVE DISCRETE MATHEMATICS by translating the letters into numbers, applying the Caesar Cipher Encryption function and then translating the numbers back into letters.
Solution:
The encrypted message will be "LORYH GLVFUHWH PDWKHPDWLFV "

(b) Decrypt these messages encrypted using the Caesar Cipher.

i) PLG WZR DVVLJQPHQW
Solution:
"MID TWO ASSIGNMENT" will be decrypted message.

ii) IDVW QXFHV XQLYHUVLWB
Solution:
"FAST NUCES UNIVERSITY "will be decrypted message.

11. (a) Which memory locations are assigned by the hashing function h(k) = k mod 97 to the records of insurance company customers with these Social Security numbers?

i) 034567981
Solution: **034567981 mod 97 = 91**

ii) 183211232
Solution: **183211232 mod 97 = 57**

iii) 220195744
Solution: **220195744 mod 97 = 21**

iv) 987255335
Solution: **987255335 mod 97 = 5**

(b) Which memory locations are assigned by the hashing function h(k) = k mod 101 to the records of insurance company customers with these Social Security numbers?
i) 104578690
Solution: **104578690 mod 101 = 58.**

ii) 432222187
Solution: **432222187 mod 101 = 60.**

iii) 372201919
Solution: **372201919 mod 101 = 32.**

iv) 501338753
Solution: **501338753 mod 101 = 3.**

12. **What sequence of pseudorandom numbers is generated using the linear congruential generator?**
$x_n+1 = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$?
Solution:
$X_1 = (4 * 3 + 1) \bmod 7 = 6.$
$X_2 = (4 * 6 + 1) \bmod 7 = 4.$
$X_3 = (4 * 4 + 1) \bmod 7 = 3.$
$X_4 = (4 * 3 + 1) \bmod 7 = 6.$
$X_5 = (4 * 6 + 1) \bmod 7 = 4$
Sequence: 6,4,3,6, 4…….

13. **(a) Determine the check digit for the UPCs that have these initial 11 digits.**

i) 73232184434
Solution:
$7*3 + 3 + 2*3 + 3 + 2*3 + 1 + 8*3 + 4 + 4*3 + 3 + 4*3 + x_{12} = 0 \bmod 10$
$21 + 3 + 6 + 3 + 6 + 1 + 24 + 4 + 12 + 3 + 12 + x_{12} = 0 \bmod 10$
$95 + x_{12} = 0 \bmod 10$ **Check digit is $x_{12} = 5$.**

ii) 63623991346
Solution:
$6*3 + 3 + 6*3 + 2 + 3*3 + 9 + 9*3 + 1 + 3*3 + 4 + 6*3 + x_{12} = 0 \bmod 10$
$18 + 3 + 18 + 2 + 9 + 9 + 27 + 1 + 9 + 4 + 18 + x_{12} = 0 \bmod 10$
$118 + x_{12} = 0 \bmod 10$ **Check digit is $x_{12} = 2$.**

(b) Determine whether each of the strings of 12 digits is a valid UPC code.

i) 036000291452
Solution:
$0*3 + 3 + 6*3 + 0 + 0*3 + 0 + 2*3 + 9 + 1*3 + 4 + 5*3 + 2 = 0 \bmod 10$
$0 + 3 + 18 + 0 + 0 + 0 + 6 + 9 + 3 + 4 + 15 + 2 = 0 \bmod 10$
$60 \equiv 0 \bmod 10$ **It's a valid UPC code.**

ii) 012345678903
Solution:
$0*3 + 1 + 2*3 + 3 + 4*3 + 5 + 6*3 + 7 + 8*3 + 9 + 0*3 + 3 = 0 \bmod 10$
$0 + 1 + 6 + 3 + 12 + 5 + 18 + 7 + 24 + 9 + 0 + 3 = 0 \bmod 10$
$88 \not\equiv 0 \bmod 10$ **It's not a valid UPC code.**

14. **(a) The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881.What is the check digit for that book?**
Solution:
$1*0 + 2*0 + 3*7 + 4*1 + 5*1 + 6*9 + 7*8 + 8*8 + 9*1 + x_{10} = 0 \bmod 11$
$0 + 0 + 21 + 4 + 5 + 54 + 56 + 64 + 9 + x_{10} = 0 \bmod 11$
$213 + x_{10} = 0 \bmod 11$ **Check digit, $x_{10} = 4$.**

(b) **The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.**
Solution:

$$\begin{aligned} x_{10} &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot Q + 9 \cdot 1 \bmod 11 \\ &= 0 + 6 + 6 + 4 + 25 + 0 + 0 + 8Q + 9 \bmod 11 \\ &= 8Q + 50 \bmod 11 \end{aligned}$$

The check digit is known to be 8.

$$8Q + 50 \bmod 11 = 8$$

Since $50 \bmod 11 = 6$

$$8Q + 6 \bmod 11 = 8$$

Subtract 6 from each side of the equation:

$$8Q \bmod 11 = 2$$

Since the inverse of $8 \bmod 11$ is $7 \bmod 11$, we should multiply both sides of the equation by 7:

$$\begin{aligned} 7 \cdot 8Q \bmod 11 &= 7 \cdot 2 \bmod 11 \\ 56Q \bmod 11 &= 14 \bmod 11 \\ Q \bmod 11 &= 3 \end{aligned}$$

Since Q is a digit (between 0 and 9), Q then has to be equal to 3.

15. **Encrypt the message ATTACK using the RSA system with n = 43 · 59 and e = 13, translating each letter into integers and grouping together pairs of integers.**
Solution:
A T T A C K
00 19 19 00 02 10

- **$n = 43 \cdot 59 = 2537$**
- **$k = (43 - 1)(59 - 1) = 2436$**
- **$e = 13$**

Encryption Function: $C = M^e \bmod n$

$C = 0019^{13} \bmod 2537$ $\qquad$ $C = 1900^{13} \bmod 2537$ $\qquad$ $C = 0210^{13} \bmod 2537$

16. **(a) An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?**
Solution:
There are 27 * 37 = 99 offices in the building.

(b) A particular brand of shirt comes in 12 colors, has a male version and a female version, and comes in three sizes for each sex. How many different types of this shirt are made?
Solution:
12 * 2 * 3 shirts are required.

17. **(a) How many different three-letter initials can people have?**
Solution:
People can have 26 *26 * 26 = 26^3 different three-letter initials.

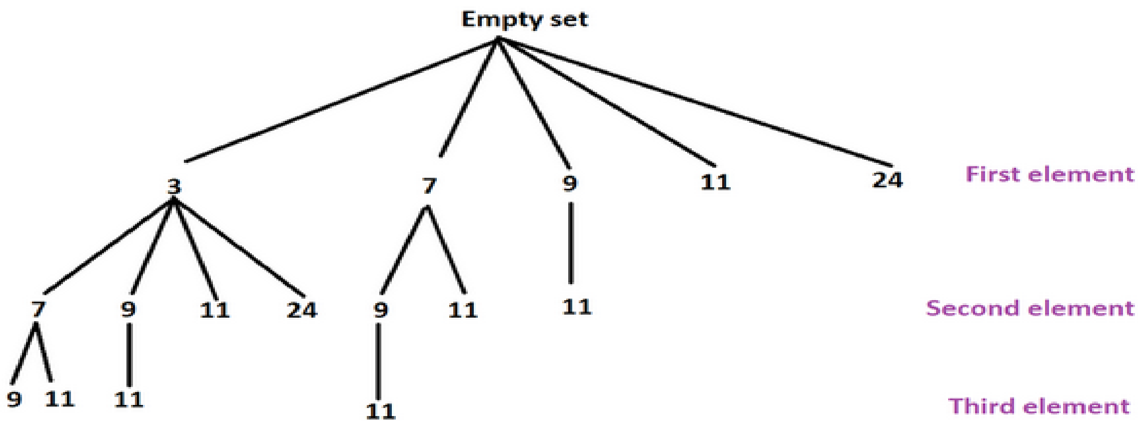
(b) How many different three-letter initials with none of the letters repeated can people have?
Solution:
People can have 26 *25 * 24 = 15,600 different three-letter initials with none of the letters repeated.

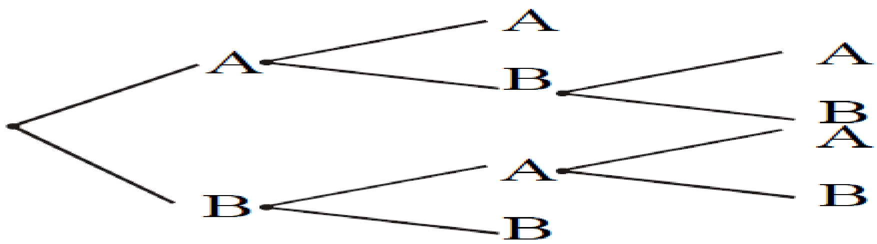
18. (a) A wired equivalent privacy (WEP) key for a wireless fidelity (WiFi) network is a string of either 10, 26, or 58 hexadecimal digits. How many different WEP keys are there?
Solution:
There are16 place values for hexadecimal numbers: 0 to 9, A, B, C, D, E and F.
So, $16^{10} + 16^{28} + 16^{58}$ different WEP keys are possible.

(b) How many strings are there of four lowercase letters that have the letter x in them?
Solution:
There would be $26^4 – 25^4$ = 66,351 strings.

19. (a) How many functions are there from the set {1, 2, . . . , *m*}, where *m* is a positive integer, to the set {0, 1}?
Solution:
Since each value of the domain can be mapped to one of two values. Number of functions are:
= 2 * 2 * 2 * 2 * ….. * m = 2^m .

(b) How many one-to-one functions are there from a set with five elements to sets with five elements?
Solution:
Each successive element from the domain will have one option than its predecessor as it is one-to-one function. So, number of functions are 5 * 4 * 3 * 2 * 1 = 120.

20. (a) Use a tree diagram to determine the number of subsets of {3, 7, 9, 11, 24} with the property that the sum of the elements in the subset is less than 28.
Solution:


(b) Teams A and B play in a tournament. The team that wins first two games wins the tournament. Use a tree diagram to find the number of possible ways in which the tournament can occur.
Solution:


21. (a) Eight members of a school marching band are auditioning for 3 drum major positions. In how many ways can students be chosen to be drum majors?
Solution:
There are ${}^{8}C_{3}$ = 56 ways to choose the students.

(b) You must take 6 CS elective courses to meet your graduation requirements at FAST-NUCES. There are 12 CS courses you are interested in. In how many ways can you select your elective Courses?
Solution:
There are ${}^{12}C_{6}$ = 924 ways to select the elective courses.

(c) Nine people in our class want to be on a 5-person basketball team to represent the class. How many different teams can be chosen?
Solution:
${}^{9}C_{5}$= 126 different teams can be selected.

22. (a) A committee of five people is to be chosen from a group of 20 people. How many different ways can a chairperson, assistant chairperson, treasurer, community advisor, and record keeper be chosen?
Solution:
There are ${}^{20}P_{5}$= 1,860,480 ways to choose a chairperson, assistant chairperson, treasurer, community advisor, and record keeper.

(b) A relay race has 4 runners who run different legs of the race. There are 16 students on your track team. In how many ways can your coach select students to compete in the race? Assume that the order in which the students run matters.
Solution:
There are ${}^{16}P_{4}$= 43,680 ways coach can select students to compete in the race.

(c) Your school yearbook has an editor in chief and an assistant editor in chief. The staff of the yearbook has 15 students. In how many ways can a student be chosen for these 2 positions?
Solution:
There are ${}^{15}P_{2}$= 210 ways student can be chosen for these 2 positions.

23. (a) A deli offers 5 different types of meat, 3 types of breads, 4 types of cheeses and 6 condiments. How many different types of sandwiches can be made of 1 meat, 2 bread, 1 cheese, and 3 condiments?
Solution:
${}^{5}C_{1} * {}^{3}C_{2} * {}^{4}C_{1} * {}^{6}C_{3}$ = 1200 Sandwiches can be made of 1 meat, 2 bread, 1 cheese, and 3 condiments.

(b) Police use photographs of various facial features to help eyewitnesses identify suspects. One basic identification kit contains 15 hairlines, 48 eyes and eyebrows, 24 noses, 34 mouths, and 28 chins and 28 cheeks. Find the total number of different faces.
Solution:
There are 15 * 48 * 24 * 34 * 28 * 28 = 460,615,680 different faces.

24. (a) How many bit strings of length 10 either begin with three 0s or end with two 0s?
Solution:
A = Strings begins with three 0s = 2^7 = 128 B = Strings end with two 0s = 2^8 = 256
$A \cap B = 2^5 = 32$
$A \cup B = A + B - A \cap B = 128 + 256 - 32 = 352$.

(b) How many bit strings of length 5 either begin with 0 or end with two 1s?
A = Strings begins with 0s = 2^4 = 16 **B = Strings end with two 1s = 2^3= 8**
$A \cap B = 2^2 = 4$
AUB = A + B – A∩B = 16 + 8 – 4 = 20.

25. (a) Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.
Solution:
The first letter of each last name are the pigeonholes, and the letters of the alphabet are pigeons. By the generalized pigeonhole principle, $\left\lceil \frac{30}{26} \right\rceil$ = 2. So there are at least two students, have last names that begin with the same letter.

(b) Assuming that no one has more than 1,000,000 hairs on the head of any person and that the population of New York City was 8,008,278 in 2010, show there had to be at least nine people in New York City in 2010 with the same number of hairs on their heads.
Solution:
By the generalized pigeonhole principle, $\left\lceil \frac{8008278}{1000000} \right\rceil$ = 9.

(c) There are 38 different time periods during which classes at a university can be scheduled. If there are 677 different classes, how many different rooms will be needed?
Solution:
The 38 time periods are the pigeonholes, and the 677 classes are the pigeons. By the generalized pigeonhole principle there is at least one time period in which at least $\left\lceil \frac{677}{38} \right\rceil$ = 18 classes are meeting. Since each class must meet in a different room, we need 18 rooms.

26. (a) What is the coefficient of x^5 in $(1 + x)^{11}$?
Solution:
From binomial theorem, it follows that coefficient is:
$^{n}C_{r} = {}^{11}C_{5} = 462$.

(b) What is the coefficient of a^7b^{17} in $(2a – b)^{24}$?
Solution:
From binomial theorem, it follows that coefficient is:
$^{n}C_{r} = {}^{24}C_{17}\,(2)^7\,(-1)^{17} = -\,44,301,312$.

27. A class has 20 women and 16 men. In how many ways can you
(a) put all the students in a row?
Solution:
There are 36 students. They can be put in a row in 36! ways.

(b) put 7 of the students in a row?
Solution:
You need to have an ordered arrangement of 7 out of 36 students. The number of such arrangements is *P* (36,7).

(c) put all the students in a row if all the women are on the left and all the men are on the right?
Solution:
You need to have an ordered arrangement of all 20 women and ordered arrangement of all 16 men. By the product rule, this can be done in 20! * 16! ways.

28. (a) Prove the statement: There is an integer n > 5 such that $2^n – 1$ is prime.
Solution:
Here we are asked to show a single integer for which $2^n – 1$ is prime. First of all we will check the integers from 1 and check whether the answer is prime or not by putting these values in $2^n – 1$. When we got the answer is prime then we will stop our process of checking the integers and we note that,
Let n = 7, then

$2^n – 1 = 2^7 – 1 = 128 – 1 = 12$
and we know that 127 is prime.

(b) Prove that for any integer a and any prime number p, if p | a, $P \nmid (a + 1)$.
Solution:
Suppose there exists an integer a and a prime number p such that p|a and p|(a+1).
Then by definition of divisibility there exist integer r and s so that
a = p·r and a + 1 = p·s
It follows that
1 = (a + 1) - a
= p·s – p·r
= p·(s – r) where s – r ∈ Z
This implies p | 1.
But the only integer divisors of 1 are 1 and -1 and since p is prime p>1. This is a contradiction. Hence the supposition is false, and the given statement is true.

29. (a) Prove the statement: There are real numbers a and b such that $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$.
Solution:
Let $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$
Squaring, we get a + b = a + b + 2 $\sqrt{a}\sqrt{b}$
⇒ $0 = 2\sqrt{a}\sqrt{b}$ cancelling a + b
⇒ $0 = 2\sqrt{ab}$
⇒ $0 = ab$ squaring
⇒ either a = 0 or b = 0
It means that if we want to find out the integers which satisfy the given condition then one of them must be zero. Hence if we let a = 0 and b = 3 then
R.H.S = $\sqrt{(a+b)} = \sqrt{0+3} = \sqrt{3}$
Now,
L.H.S = $\sqrt{0} + \sqrt{3} = \sqrt{3}$
From above it quite clear that the given condition is satisfied if we take a=0 and b=3.

(b) Prove that if $|x| > 1$ then $x > 1$ or $x < -1$ for all $x \in R$.
Solution:

The contrapositive statement is:
if $x \leq 1$ and $x \geq -1$ then $|x| \leq 1$ for $x \in R$.
Suppose that $x \leq 1$ and $x \geq -1$
$\Rightarrow x \leq 1$ and $x \geq -1$
$\Rightarrow -1 \leq x \leq 1$
and so
$|x| \leq 1$
Equivalently $|x| > 1$.

30. (a) Find a counter example to the proposition: For every prime number n, n + 2 is prime.

<u>SOLUTION:</u>

Let the prime number n be 7, then
$n + 2 = 7 + 2 = 9$
which is not prime.

(b) Show that the set of prime numbers is infinite.
Solution:

Suppose the set of prime numbers is finite.
Then, all the prime numbers can be listed, say, in ascending order:
$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots,\ p_n$
Consider the integer
$N = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1$

Then $N > 1$. Since any integer greater than 1 is divisible by some prime number p, therefore $p \mid N$.
Also since p is prime, p must equal one of the prime numbers
$p_1, p_2, p_3, \cdots, p_n$.
Thus
$P \mid (p_1, p_2, p_3, \cdots, p_n)$

But then
$P \nmid (p_1, p_2, p_3, \cdots, p_n + 1)$

So $P \nmid N$

Thus $p \mid N$ and $p \nmid N$, which is a contradiction.

Hence the supposition is false and the theorem is true.

31. (a) Prove by contradiction method, the statement: If n and m are odd integers, then n + m is an even integer.
Solution:
Suppose n and m are odd and n + m is not even (odd i.e by taking contradiction).
Now $n = 2p + 1$ for some integer p
and $m = 2q + 1$ for some integer q
Hence $n + m = (2p + 1) + (2q + 1)$
$= 2p + 2q + 2 = 2 \cdot (p + q + 1)$
which is even, contradicting the assumption that n + m is odd.

(b) Prove the statement by contraposition: For all integers m and n, if m + n is even then m and n are both even or m and n are both odd.

Solution:

"For all integers m and n, if m and n are not both even and m and n are not both odd, then m + n is not even."

Or more simply,

"For all integers m and n, if one of m and n is even and the other is odd, then m + n is odd"

Suppose m is even and n is odd. Then

	$m = 2p$	for some integer p
and	$n = 2q + 1$	for some integer q
Now	$m + n = (2p) + (2q + 1)$	
	$= 2\cdot(p + q) + 1$	
	$= 2\cdot r + 1$ where $r = p + q$ is an integer	

Hence m + n is odd.

Similarly, taking m as odd and n even, we again arrive at the result that m + n is odd.

Thus, the contrapositive statement is true. Since an implication is logically equivalent to its contrapositive so the given implication is true.

32. (a) Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.

Solution:

Suppose $6-7\sqrt{2}$ is rational.

Then by definition of rational,

$$6-7\sqrt{2}=\frac{a}{b}$$

for some integers a and b with $b\neq 0$.

Now consider,

$$7\sqrt{2}=6-\frac{a}{b}$$

$$\Rightarrow \quad 7\sqrt{2}=\frac{6b-a}{b}$$

$$\Rightarrow \quad \sqrt{2}=\frac{6b-a}{7b}$$

Since a and b are integers, so are 6b-a and 7b and $7b\neq 0$;

hence $\sqrt{2}$ is a quotient of the two integers 6b-a and 7b with $7b\neq 0$.

Accordingly, $\sqrt{2}$ is rational (by definition of rational).

This contradicts the fact because $\sqrt{2}$ is irrational.

Hence our supposition is false and so $6-7\sqrt{2}$ is irrational.

(b) Prove by contradiction that $\sqrt{2}$ + $\sqrt{3}$ is irrational.
Solution:

Suppose $\sqrt{2}+\sqrt{3}$ is rational. Then, by definition of rational, there exists integers a and b with b≠0 such that

$$\sqrt{2}+\sqrt{3}=\frac{a}{b}$$

Squaring both sides, we get

$$2+3+2\sqrt{2}\sqrt{3}=\frac{a^2}{b^2}$$

$$\Rightarrow \qquad 2\sqrt{2\times 3}=\frac{a^2}{b^2}-5$$

$$\Rightarrow \qquad 2\sqrt{6}=\frac{a^2-5b^2}{b^2}$$

$$\Rightarrow \qquad \sqrt{6}=\frac{a^2-5b^2}{2b^2}$$

Since a and b are integers, so are therefore $a^2 - 5b^2$ and $2b^2$ with $2b^2 \neq 0$. Hence $\sqrt{6}$ is the quotient of two integers $a^2 - 2b^2$ and $2b^2$ with $2^2 \neq 0$. Accordingly, $\sqrt{6}$ is rational. But this is a contradiction, since $\sqrt{6}$ is not rational. Hence our supposition is false and so $\sqrt{2}+\sqrt{3}$ is irrational.

<u>**REMARK:**</u>

The sum of two irrational numbers need not be irrational in general for

$$(6-7\sqrt{2})+(6+7\sqrt{2})=6+6=12$$

which is rational.

33. By mathematical induction, prove that following is true for all positive integral values of n.

(a) $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = (n(n+1)(2n+1))/6$

SOLUTION:

Let P(n) denotes the given equation

1. **Basis step:**

P(1) is true

For n = 1

L.H.S of P(1) = 12 = 1

$$\text{R.H.S of P(1)} = \frac{1(1+1)(2(1)+1)}{6}$$

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

So L.H.S = R.H.S of P(1).Hence P(1) is true

2.Inductive Step:

Suppose P(k) is true for some integer k ≥1;

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6} \qquad \ldots\ldots\ldots(1)$$

To prove P(k+1) is true; i.e.;

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+1+1)(2(k+1)+1)}{6} \qquad \ldots(2)$$

Consider LHS of above equation (2)

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= (k+1)\left[\frac{k(2k+1)}{6} + (k+1)\right]$$

$$= (k+1)\left[\frac{k(2k+1) + 6(k+1)}{6}\right]$$

$$= (k+1)\left[\frac{2k^2 + k + 6k + 6}{6}\right]$$

$$= \frac{(k+1)(2k^2 + 7k + 6)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$$= \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$$

(b) $1+2+2^2 + \dots + 2^n = 2^{n+1} - 1$ for all integers $n \geq 0$

SOLUTION:

Let P(n): $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$

1. **Basis Step:**

P(0) is true.

For $n = 0$
L.H.S of $P(0) = 1$
R.H.S of $P(0) = 2^{0+1} - 1 = 2 - 1 = 1$
Hence P(0) is true.

2. **Inductive Step:**

Suppose P(k) is true for some integer $k \geq 0$; i.e.,

$$1+2+2^2+\dots+2^k = 2^{k+1} - 1 \dots\dots\dots\dots(1)$$

To prove P(k+1) is true, i.e.,

$$1+2+2^2+\dots+2^{k+1} = 2k+1+1 - 1 \dots\dots\dots\dots(2)$$

Consider LHS of equation (2)

$$\begin{aligned} 1+2+2^2+\dots+2^{k+1} &= (1+2+2^2+\dots+2^k) + 2^{k+1} \\ &= (2^{k+1} - 1) + 2^{k+1} \\ &= 2\cdot 2^{k+1} - 1 \\ &= 2^{k+1+1} - 1 = \text{R.H.S of (2)} \end{aligned}$$

Hence P(k+1) is true and consequently by mathematical induction the given propositional function is true for all integers $n \geq 0$.

(c) $1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4} n^2(n + 1)^2$

Solution:

1. Show it is true for n=1

$1^3 = \frac{1}{4} \times 1^2 \times 2^2$ is True

2. Assume it is true for n=k

$1^3 + 2^3 + 3^3 + \dots + k^3 = \frac{1}{4}k^2(k + 1)^2$ is True (An assumption!)

Now, prove it is true for "k+1"

$1^3 + 2^3 + 3^3 + \dots + (k + 1)^3 = \frac{1}{4}(k + 1)^2(k + 2)^2$

We know that $1^3 + 2^3 + 3^3 + \dots + k^3 = \frac{1}{4}k^2(k + 1)^2$ (the assumption above), so we can do a replacement for all but the last term:

$\frac{1}{4}k^2(k + 1)^2 + (k + 1)^3 = \frac{1}{4}(k + 1)^2(k + 2)^2$

Multiply all terms by 4:

$k^2(k + 1)^2 + 4(k + 1)^3 = (k + 1)^2(k + 2)^2$

All terms have a common factor $(k + 1)^2$, so it can be canceled:

$k^2 + 4(k + 1) = (k + 2)^2$

And simplify:

$k^2 + 4k + 4 = k^2 + 4k + 4$

They are the same! So it is true.

So:

$1^3 + 2^3 + 3^3 + \dots + (k + 1)^3 = \frac{1}{4}(k + 1)^2(k + 2)^2$ is True.

34. As we have discussed, the practical application of all the topics in the class. Now you are required to submit at least two real world applications of the following topics.

(a) Combination
(b) Permutations
(c) Binomial Theorem
(d) Proof methods
(e) Mathematical Induction