UTS

SEAT NUMBER:

STUDENT NUMBER:

SURNAME:
(FAMILY NAME)

OTHER NAMES:

This paper and all materials issued must be returned at the end of the examination.
They are not to be removed from the exam centre.

Examination Conditions:

It is your responsibility to fill out and complete your details in the space provided on all the examination material provided to you. Use the time before your examination to do so as you will not be allowed any extra time once the exam has ended.

You are **not** permitted to have on your desk or on your person any unauthorised material. This includes but not limited to:

- Mobile phones
- Smart watches and bands
- Electronic devices
- Draft paper (unless provided)
- Textbooks (unless specified)
- Notes (unless specified)

You are **not** permitted to obtain assistance by improper means or ask for help from or give help to any other person.

If you wish to **leave and be re-admitted** (including to use the toilet), you have to wait until **90 mins** has elapsed.

If you wish to **leave the exam room permanently**, you have to wait until **60 mins** has elapsed.

You are not permitted to leave your seat (including to use the toilet) during the final 15 mins.

During the examination **you must first seek permission** (by raising your hand) from a supervisor before:

- Leaving early
- Using the toilet
- Accessing your bag

Misconduct action will be taken against you if you breach university rules.

Declaration: I declare that I have read the advice above on examination conduct and listened to the examination supervisor's instructions for this exam. In addition, I am aware of the university's rules regarding misconduct during examinations. I am not in possession of, nor do I have access to, any unauthorised material during this examination. I agree to be bound by the university's rules, codes of conduct, and other policies relating to examinations.

Signature:

Date:

37181 Discrete Mathematics

Time Allowed: 120 minutes.

Reading time: 10 minutes.

Reading time is for reading only. You are not permitted to write, calculate or mark your paper in any way during reading time.

Restricted Open Book: Four A4 pages written (handwritten or typed) on both sides allowed. Please ensure to write your name and student ID number on the top of each page (do this before entering the exam).

Permitted materials for this exam:

Non-programmable Calculator
Four A4 pages written (handwritten or typed) on both sides.

Materials provided for this exam:

1 x 8 Page Booklet
1 x General Purpose Answer Sheets (GPAS-240R)

Students please note:

All questions are multiple choice. Make sure you fill in the GPAS sheet very carefully, as per the instructions. If you make a mistake, ask for a replacement GPAS sheet.

Also circle your correct response to each question in the exam booklet. Only the GPAS sheets will be marked, but if there is any problem with the machine this may help as a backup only.

The 8 page booklet is for rough working out.

Submit all materials at the end of the exam, including your 4 pages of notes.

Each question answer is worth 1 mark, total 27 marks.

Do not open your exam paper until instructed.

Rough work space
Do **not** write your answers on this page.

Choose the correct answer and mark it clearly on the GPAS sheet. Also clearly indicate your choice on this exam paper as a back-up. Each question is worth 1 mark.

1. Let p, s be statements. The final column of the truth table for

$$s \leftrightarrow (p \rightarrow ((\neg p) \vee s))$$

is

A.

p	s	$s \leftrightarrow (p \rightarrow ((\neg p) \vee s))$
1	1	1
1	0	1
0	1	1
0	0	1

B.

p	s	$s \leftrightarrow (p \rightarrow ((\neg p) \vee s))$
1	1	1
1	0	1
0	1	1
0	0	0

C.

p	s	$s \leftrightarrow (p \rightarrow ((\neg p) \vee s))$
1	1	1
1	0	0
0	1	1
0	0	0

D.

p	s	$s \leftrightarrow (p \rightarrow ((\neg p) \vee s))$
1	1	0
1	0	1
0	1	1
0	0	0

E. none of (A)–(D).

2. Consider the following pseudocode:

```
procedure (n int)
while n>0
      n := floor(n/2)
      print n
endwhile
```

On input $n \in \mathbb{N}$, the number of times the line `print n` is executed is roughly[1]

A. $n + \text{const}$

B. $n^2 + \text{const}$

C. $n! + \text{const}$

D. $\log_2 n + \text{const}$

E. none of the above.

[1] here const denotes a constant term

3. Consider the following statement and proof.

Lemma 1. *For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Suppose $a, b, c \in \mathbb{Z}$ and $a \mid b$ and $b \mid c$.

By definition, this means $\exists\ r, s \in \mathbb{Z}$ with $b = ar$ and $c = bs$.

Then $c = bs = (ar)s = a(rs)$.

Thus, $a \mid c$ by definition of divisibility and this is what was to be shown. $\square$

The proof style used in this proof is

A. contrapositive

B. induction

C. contradiction

D. direct

E. none of (A)–(D).

4. Fill in the missing box in the following statement and proof.

Lemma 2. *Let $q \in \mathbb{Z}$. If q is not divisible by 3, then $q^2 \equiv_3 1 \mod 3$.*

Proof. If q is not divisible by 3 then $\exists n \in \mathbb{Z}$ and $i \in \{1,2\}$ such that $q = 3n + i$.
Then $q^2 = 9n^2 + 6ni + i^2 = 3(3n^2 + 2ni) + i^2 \equiv i^2 \mod 3$.

If $i = 1$ then $i^2 = 1$, and if $\boxed{}$
so the result follows by transitivity of the relation $\equiv \mod 3$. □

A. contrapositive

B. $i = 2$ then $i^2 = 4 \equiv 1 \mod 3$

C. $i \neq 2$ then $i^2 = 1$

D. $i = 2$ then $i^2 \equiv 0 \mod 3$

E. none of (A)–(D).

5. The negation of the statement "every non-empty subset of $\mathbb{N}$ has a first element" is

A. every subset of $\mathbb{N}$ is either empty or does not have a first element

B. there exists a subset of $\mathbb{N}$ which is empty

C. if s, t are first elements of a non-empty set $S \subseteq \mathbb{N}$ then $s = t$

D. there is some subset of $\mathbb{N}$ which is non-empty and does not have a first element

E. none of (A)–(D).

6. Let $A, B \in \mathscr{U}$ be particular but arbitrary sets. The <u>complement</u> of the set

$$\emptyset \cup \overline{A \cap (\overline{B} \cup A)}$$

is equal to

A. $\emptyset$

B. $\overline{B} \cap A$

C. $A \cup (\overline{A} \cap B)$

D. A

E. none of (A)–(D).

7. Consider the statement

$$\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\, [(xy > 0) \vee (x > 0) \vee (y > 0) \vee (x = 0)]\,.$$

Which of the following is true?

A. putting $x = 1, y = 0$ shows that the statement is false

B. the statement is true because if $x > 0$ it is true and if $x < 0$ we can take $y < 0$

C. putting $x = -1, y = 0$ shows that the statement is false

D. putting $x = -1, y = -1$ shows that the statement is false

E. none of (A)–(D).

8. The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2 - 5$ is

   A. onto and not one-to-one

   B. not one-to-one and not onto

   C. a bijection

   D. one-to-one and not onto

   E. none of (A)–(D).

9. Let $A, B \in \mathscr{U}$ be sets. A *relation* from A to B is

   A. an element of $\mathscr{P}(A \times B)$

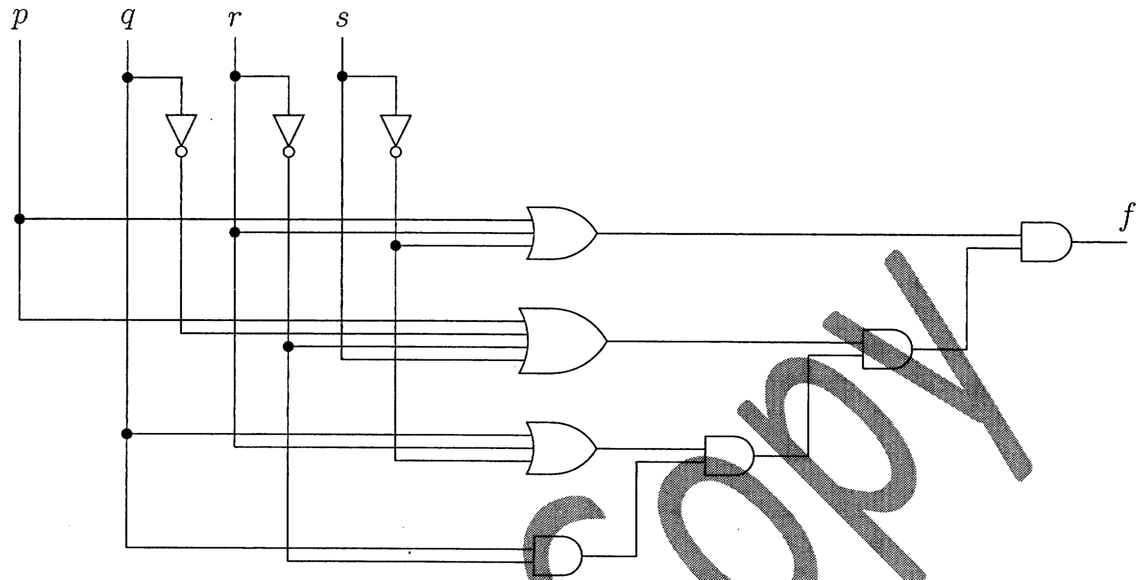
   B. a non-empty subset of $A \times B$

   C. a function from A to B that it not one-to-one

   D. an element of $\mathscr{P}(A \cup B)$

   E. none of (A)–(D).

10. Consider the logic circuit



On which of the following inputs is the output at f 1?

A. $p = 0, q = 0, r = 0, s = 0$

B. $p = 1, q = 0, r = 0, s = 0$

C. $p = 0, q = 1, r = 0, s = 0$

D. $p = 0, q = 0, r = 1, s = 0$

E. none of (A)–(D).

11. The pre-order traversal of the rooted tree encoding

$$\frac{b+7f}{e(2+c)}$$

is

A. $b\ +\ 7\ \div\ e\ \times\ 2\ \times\ f\ +\ c$

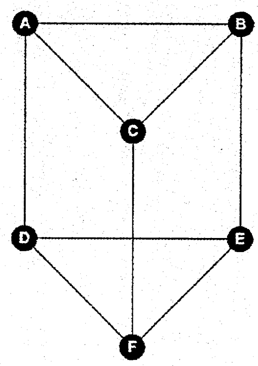
B. $b\ 7\ e\ 2\ +\ f\ \times\ c\ \times\ +\ \div$

C. $\div\ +\ b\ \times\ 7\ f\ \times\ e\ +\ 2\ c$

D. $\div\ +\ b\ \times\ 7\ f\ e\ \times\ +\ 2\ c$

E. none of (A)–(D).

12. The graph



A. has an Euler path

B. is simple and bipartite

C. has a spanning tree containing 6 edges

D. has a spanning tree containing 5 edges

E. none of (A)–(D).

13. Let G be the undirected graph with adjacency matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The number of paths of length 5 from any vertex of G to itself is

A. 5

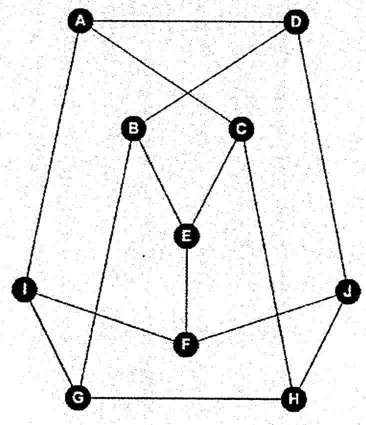
B. 0

C. 1

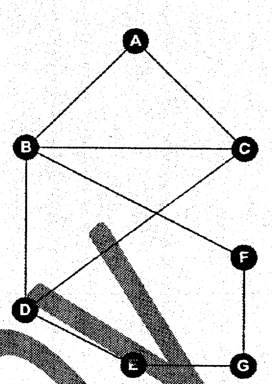
D. 2

E. the answer is different depending on which vertex is chosen.

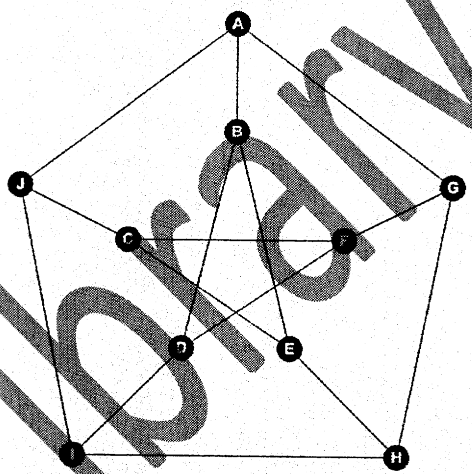
14. Which of the following graphs has a Hamilton cycle?



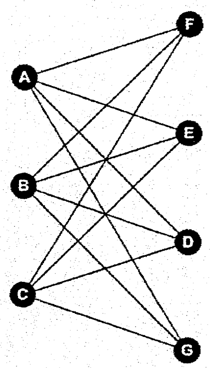
A.



B.



C.



D.

E. none of (A)–(D).

15. The number of non-isomorphic trees with 4 vertices is

A. 2

B. 1

C. 3

D. 4

E. none of (A)–(D).

16. The number of edges in a graph with degree sequence $2, 2, 2, 3, 3, 3, 4$ is

A. 8

B. 10

C. 9

D. 11

E. no graph exists with this degree sequence.

17. Define a function $A : \mathbb{N}^2 \to \mathbb{N}$ using the following recursive definition.

$$\begin{aligned} A(0,n) &= n+1 && n \geq 0, \\ A(m,0) &= A(m-1,1) && m > 0, \\ A(m,n) &= A(m-1, A(m,n-1)) && m,n > 0. \end{aligned}$$

Then $A(2,1)$ is equal to

A. 4

B. 7

C. 6

D. 5

E. none of (A)–(D).

18. Which of the following is not a loop invariant for the while loop within the following segment of pseudocode:

```
procedure (n int, j int)

while n>0
      n := n - 2*j
      print n
endwhile
```

A. nj is odd

B. $n > j$

C. $n + j$ is odd

D. $n + j$ is even

E. none of (A)–(D).

19. Using repeated squaring, or otherwise, the remainder of 2^{431} on division by 31 is

A. 30

B. 1

C. 2

D. 4

E. none of (A)–(D).

20. Let ϕ denote Euler's phi function. $\phi(36) =$

A. 4

B. 12

C. 16

D. 8

E. none of (A)–(D).

21. Let $\mathscr{L}$ be the relation on $\mathbb{N}$ defined by

$$a\mathscr{L}b \quad \text{if} \quad a < b \quad \text{or} \quad 5 \mid (b-a)$$

So for example $(1,6) \in \mathscr{L}$ and $(6,1) \in \mathscr{L}$. Which of the following statements is true?

A. $\mathscr{L}$ is antisymmetric

B. $\mathscr{L}$ is symmetric

C. $\mathscr{L}$ is transitive

D. $\mathscr{L}$ is reflexive

E. none of (A)–(D).

22. Let the universe of discourse be $\mathbb{N}$. Let $P(n)$ be the statement "$n^2 + 5n + 1$ is even". Which of the following statements is true?

A. $P(n)$ is true for all $n \geq 3$

B. $\exists k$ such that $P(n)$ is true for all $n \geq k$

C. $\forall k$, if $n > k$ then $P(n)$ is true

D. $\forall k$, if $P(k)$ is true then $P(k+1)$ is true

E. none of (A)–(D).

23. Using the Euclidean algorithm, or otherwise, $\gcd(480, 38) =$

A. 1

B. 2

C. 4

D. 19

E. none of (A)–(D).

24. The statement

$$\neg\,(p \wedge (q \vee r))$$

is logically equivalent to

A. $\neg(p \vee \neg q) \wedge \neg r)$

B. $\neg p \wedge (\neg q \vee \neg r)$

C. $p \wedge (\neg q \wedge \neg r)$

D. $\neg p \vee (\neg q \wedge \neg r)$

E. none of (A)–(D).

25. Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by the recursive definition

$$\begin{aligned} f(0) &= 1 \\ f(n) &= n(f(n-1)+1) \qquad n > 0. \end{aligned}$$

The value of $f(3)$ is

A. 21

B. 15

C. 28

D. 6

E. none of (A)–(D).

26. Which of the following statements is true?

    A. $n \in O(\log_2 n)$

    B. $n! \in O(n \log_2 n)$

    C. $n^4 \log_2 n \in O(n^2)$

    D. $n \log_4 n \in O(n^2)$

    E. none of (A)–(D).

27. Alice constructs an RSA system by choosing $n = 74$ and $e = 5$. Her corresponding value for d is

A. $d = 15$

B. $d = 36$

C. $d = 7$

D. $d = 17$

E. none of (A)–(D).

END OF EXAMINATION