

AMBEDKAR COLLEGE OF ARTS AND SCIENCE, WANDOOR
MAT5EJ302(1)—Data Structures and Algorithms

(2024 Admission onwards)

ANSWER KEY

Section A

(2 marks each; Ceiling 16)

1. $2 \equiv -1 \pmod{3}$, so $2^{2006} \equiv (-1)^{2006} \pmod{3}$. Since 2006 is even, $(-1)^{2006} = 1$. Hence $2^{2006} \equiv \mathbf{1} \pmod{3}$.
2. $84 = 2 \cdot 30 + 24$; $30 = 1 \cdot 24 + 6$; $24 = 4 \cdot 6 + 0$. Last non-zero remainder: $\gcd(84, 30) = \mathbf{6}$.
3. $43 = 3 \cdot 12 + 7 \equiv 7 \pmod{12}$; $61 = 5 \cdot 12 + 1 \equiv 1 \pmod{12}$. So $(43 \times 61) \bmod 12 \equiv 7 \times 1 = \mathbf{7} \pmod{12}$.

4. An integer N needs about $\log_2 N$ bits in binary and about $\log_{10} N$ digits in decimal. Their ratio is

$$\frac{\log_2 N}{\log_{10} N} = \log_2 10 \approx 3.32$$

(change of base), independent of N . Since $3.32 < 4$, the binary form is at most about four times as long. For very large numbers the exact ratio is $\log_2 10 \approx 3.32$.

5. If N has n bits then $N \approx 2^n$, so $\sqrt{N} \approx 2^{n/2}$. Checking every candidate divisor up to $\sqrt{N}$ performs about $\sqrt{N} = 2^{n/2}$ divisions, which grows exponentially with the input size n (every extra two bits of N roughly doubles the work).
6. $T(n) = T(n/2) + \Theta(1)$, with solution $T(n) = \Theta(\log n)$ (Master Theorem: $a = 1$, $b = 2$, $d = 0 = \log_2 1$, Case 2).
7. $a = 8$, $b = 2$, $d = 3$. Since $\log_2 8 = 3 = d$, this is **Case 2**, so $T(n) = \Theta(\mathbf{n^3 \log n})$.
8. (a) Adjacency matrix: $\Theta(n^2)$ space. (b) Adjacency list: $\Theta(n + m)$ space.
9. $\sum_v \deg(v) = 2|E|$ is an even number. A sum of integers has the same parity as the number of odd terms it contains (each even term does not change the parity; each odd term flips it). Since the sum is even, the number of odd terms — that is, the number of odd-degree vertices — must be even.
10. A DAG is a directed graph that contains no directed cycle. Equivalent characterisation: a depth-first search of the graph produces **no back edges** (a directed graph has a cycle if and only if DFS finds a back edge).

Section B

(6 marks each; Ceiling 24)

1. Criterion: a has a multiplicative inverse modulo N if and only if $\gcd(a, N) = 1$.

5 mod 23: $\gcd(5, 23) = 1$, so an inverse exists. Euclid: $23 = 4 \cdot 5 + 3$, $5 = 1 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$. Back-substitute:

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(23 - 4 \cdot 5) - 5 = 2 \cdot 23 - 9 \cdot 5.$$

So $5^{-1} \equiv -9 \equiv 14 \pmod{23}$. Check: $5 \cdot 14 = 70 = 3 \cdot 23 + 1 \equiv 1 \pmod{23}$.

21 mod 91: $91 = 4 \cdot 21 + 7$, $21 = 3 \cdot 7 + 0$, so $\gcd(21, 91) = 7 \neq 1$. **No inverse exists.**

20 mod 79: $\gcd(20, 79) = 1$. Euclid: $79 = 3 \cdot 20 + 19$, $20 = 1 \cdot 19 + 1$. Back-substitute:

$$1 = 20 - 19 = 20 - (79 - 3 \cdot 20) = 4 \cdot 20 - 79.$$

So $20^{-1} \equiv 4 \pmod{79}$. Check: $20 \cdot 4 = 80 \equiv 1 \pmod{79}$.

2. 31 is prime, so by Fermat's Little Theorem $a^{30} \equiv 1 \pmod{31}$ whenever 31 does not divide a .

For $5^{30,000}$: $30,000 = 30 \times 1000$, so $5^{30,000} = (5^{30})^{1000} \equiv 1^{1000} = 1 \pmod{31}$.

For $6^{123,456}$: $123,456 = 30 \times 4115 + 6$, so $6^{123,456} = (6^{30})^{4115} \cdot 6^6 \equiv 6^6 \pmod{31}$. Now $6^2 = 36 \equiv 5$, $6^4 \equiv 25$, $6^6 \equiv 25 \cdot 5 = 125 = 4 \cdot 31 + 1 \equiv 1 \pmod{31}$.

Hence $5^{30,000} - 6^{123,456} \equiv 1 - 1 = 0 \pmod{31}$. **Yes**, the difference is a multiple of 31.

3. (a) Fermat's Little Theorem: if p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

(b) $N = 15$, $a = 2$: $2^4 = 16 \equiv 1 \pmod{15}$, so $2^{14} = 2^{4 \cdot 3 + 2} \equiv 2^2 = 4 \not\equiv 1 \pmod{15}$. The test fails, so 15 is **composite** and 2 is a witness to its compositeness.

$N = 17$, $a = 2$: $2^4 \equiv -1$, so $2^8 \equiv 1$ and $2^{16} \equiv 1 \pmod{17}$. The test **passes**, consistent with 17 being prime.

(c) A *Fermat liar* is a base a coprime to a composite N for which $a^{N-1} \equiv 1 \pmod{N}$ — it wrongly suggests N is prime. A *Carmichael number* is a composite N (e.g. 561) for which every a coprime to N is a Fermat liar, so the Fermat test never detects its compositeness.

4. Adjacency lists (alphabetical): $A: BD$, $B: AC$, $C: BE$, $D: AE$, $E: CDF$, $F: E$.

DFS from A : $A(1) \rightarrow B(2) \rightarrow C(3) \rightarrow E(4) \rightarrow D(5)$; at D , the neighbour A is already visited and active (an ancestor, not D 's parent), giving a back edge $D-A$; D has no other neighbour, so $\text{post}(D) = 6$. Back at E , visit $F(7)$, $\text{post}(F) = 8$, $\text{post}(E) = 9$, $\text{post}(C) = 10$, $\text{post}(B) = 11$. Finally A 's other neighbour D is already finished (same edge already classified), so $\text{post}(A) = 12$.

vertex	A	B	C	D	E	F
pre	1	2	3	5	4	7
post	12	11	10	6	9	8

Tree edges: $A-B$, $B-C$, $C-E$, $E-D$, $E-F$ (5 edges). Back edge: $A-D$ (1 edge). Total = 6 edges, matching the graph. Connected components: **1** (all six vertices lie in a single DFS tree).

5. **Algorithm A:** $T(n) = 5T(n/2) + \mathcal{O}(n)$, so $a = 5$, $b = 2$, $d = 1$. Since $\log_2 5 \approx 2.32 > 1$, Case 3 gives $T(n) = \Theta(n^{\log_2 5}) \approx \Theta(n^{2.32})$.

Algorithm B: $T(n) = 2T(n-1) + \mathcal{O}(1)$. This is subtractive, so the Master Theorem does not apply; expand:

$$T(n) \leq 2T(n-1) + c \leq 4T(n-2) + 3c \leq \dots \leq 2^k T(n-k) + c(2^k - 1).$$

At $k = n-1$ (base case), $T(n) = \Theta(2^n)$ — **exponential**.

Algorithm C: $T(n) = 9T(n/3) + \mathcal{O}(n^2)$, so $a = 9$, $b = 3$, $d = 2$. Since $\log_3 9 = 2 = d$, Case 2 gives $T(n) = \Theta(n^2 \log n)$.

Choice: $\Theta(n^2 \log n)$ grows more slowly than $\Theta(n^{2.32})$ (a fixed power of n beats any power of $\log n$), and both are far better than the exponential Algorithm B. **Choose Algorithm C.**

6. $x = 1110_2 = 14$, $y = 1011_2 = 11$; $n = 4$. Halves: $x_L = 11_2 = 3$, $x_R = 10_2 = 2$, $y_L = 10_2 = 2$, $y_R = 11_2 = 3$.

$$P_1 = x_L y_L = 3 \cdot 2 = 6, \quad P_2 = x_R y_R = 2 \cdot 3 = 6,$$

$$P_3 = (x_L + x_R)(y_L + y_R) = 5 \cdot 5 = 25.$$

$$xy = P_1 2^n + (P_3 - P_1 - P_2) 2^{n/2} + P_2 = 6 \cdot 16 + 13 \cdot 4 + 6 = 96 + 52 + 6 = \mathbf{154}.$$

In binary, $154 = 10011010_2$. (Check: $14 \times 11 = 154$.)

Section C

(answer any one; 10 marks)

1. (a) $47 = 32 + 8 + 4 + 2 + 1$, so in binary $47 = \mathbf{101111}_2$.

(b) Successive squaring modulo 25:

$$9^1 \equiv 9, \quad 9^2 \equiv 81 \equiv 6, \quad 9^4 \equiv 6^2 = 36 \equiv 11,$$

$$9^8 \equiv 11^2 = 121 \equiv 21, \quad 9^{16} \equiv 21^2 = 441 \equiv 16, \quad 9^{32} \equiv 16^2 = 256 \equiv 6 \pmod{25}.$$

Since $47 = 32 + 8 + 4 + 2 + 1$ (the bit for 16 is 0, so 9^{16} is not used),

$$9^{47} \equiv 9^{32} \cdot 9^8 \cdot 9^4 \cdot 9^2 \cdot 9^1 \equiv 6 \cdot 21 \cdot 11 \cdot 6 \cdot 9 \pmod{25}.$$

Combining left to right: $6 \cdot 21 = 126 \equiv 1$; $1 \cdot 11 = 11$; $11 \cdot 6 = 66 \equiv 16$; $16 \cdot 9 = 144 \equiv 19 \pmod{25}$. So $9^{47} \equiv \mathbf{19} \pmod{25}$.

(Check via Euler's theorem: $\varphi(25) = 20$ and $\gcd(9, 25) = 1$, so $9^{47} \equiv 9^{47 \bmod 20} = 9^7 \pmod{25}$; direct computation gives $9^7 \equiv 19 \pmod{25}$ too.)

(c) If y has n bits, the method computes $9^1, 9^2, 9^4, \dots, 9^{2^{n-1}}$ by squaring, which takes $n-1$ modular squarings; it then multiplies together the powers corresponding to the (at most n) set bits of y , which takes at most $n-1$ further modular multiplications (the first selected power needs no combining multiplication). So the total is $O(n)$ modular multiplications — i.e. $O(\log y)$ — compared with the $y-1 \approx 2^n$ multiplications of the naive method, which is exponential in n .

2. Adjacency lists (alphabetical): $A:BC$, $B:D$, $C:DE$, $D:F$, $E:F$, $F:G$, $G:-$.

DFS from A : $A(1) \rightarrow B(2) \rightarrow D(3) \rightarrow F(4) \rightarrow G(5)$, $\text{post}(G) = 6$, $\text{post}(F) = 7$, $\text{post}(D) = 8$, $\text{post}(B) = 9$. Back at A , visit $C(10)$; its neighbour D is already finished ($\text{pre}(D) = 3 < \text{pre}(C) = 10$ and D is not an ancestor of C), giving a *cross edge* $C \rightarrow D$; then visit $E(11)$; its neighbour F is already finished, giving another cross edge $E \rightarrow F$; $\text{post}(E) = 12$, $\text{post}(C) = 13$, $\text{post}(A) = 14$. Every vertex is reached from A , so no further restart is needed.

(a)

vertex	A	B	C	D	E	F	G
pre	1	2	10	3	11	4	5
post	14	9	13	8	12	7	6

(b) Tree edges: $A \rightarrow B$, $A \rightarrow C$, $B \rightarrow D$, $C \rightarrow E$, $D \rightarrow F$, $F \rightarrow G$ (6 edges). Cross edges: $C \rightarrow D$ and $E \rightarrow F$ (2 edges). No back or forward edges.

(c) Sources (no incoming edge): **A** only. Sinks (no outgoing edge): **G** only.

(d) Listing vertices by decreasing post-number:

$$A(14), C(13), E(12), B(9), D(8), F(7), G(6),$$

giving the topological order **A, C, E, B, D, F, G**. (Check: every edge $A \rightarrow B$, $A \rightarrow C$, $B \rightarrow D$, $C \rightarrow D$, $C \rightarrow E$, $D \rightarrow F$, $E \rightarrow F$, $F \rightarrow G$ points forward in this order.)