CS2020A Discrete Mathematics

Aug-Dec 2025 | First Test Answer Key | 20 points

IIT Palakkad

1. Prove **Bezout's Identity.** If a and b are two relatively prime integers, then there exists two integers α and β such that $\alpha a + \beta b = 1$. (4 points)

   - Let S be the set of **positive integers** that can be expressed as an integer linear combination of a and b.
   - Since a and b are relatively prime, both cannot be 0. Hence we can assume that $a \neq 0$. If $a > 0$, then $1a + 0b = a \in S$ and if $a < 0$, $-1a + 0b = -a \in S$. So S is non-empty.
   - By Well Ordering Principle, any non-empty subset of natural numbers has a least element. Hence S has a least element. Denote it by d. We will complete the proof by showing that $d = 1$.
   - Since d is in S, there are two integers α and β such that $\alpha a + \beta b = d$.
   - Let $a = dq + r$ where q is an integer and $0 \leq r \leq d - 1$. Now $r = a - dq = a - (\alpha a + \beta b)q = (1 - \alpha q)a - (\beta q)b$ and hence r is an integer linear combination of a and b.
   - If $r > 0$, then it contradicts the minimality of d in S. Hence $r = 0$ and therefore d divides a.
   - Similarly d divides b and hence d is a common factor of a and b.
   - Since a and b are relatively prime, the only positive common factor is 1. Hence $d = 1$.

2. Using Bézout's identity, prove the following Lemma. (Do not use the Fundamental Theorem of Arithmetic in the proof.)

   Euclid's Lemma. If p is a prime and a and b are integers such that p divides ab, then p divides at least one of a or b. (2 points)

   - If p divides a, the conclusion of the lemma is true.
   - Otherwise p is not a factor of a and since the only factors of a prime number p are 1 and p, a and p are relatively prime.
   - By Bézout's identity, there exists two integers α and β such that $\alpha a + \beta p = 1$.
   - Multiplying by b on both sides we get $\alpha ab + \beta pb = b$. Since both ab and pb are multiples of p, the RHS b is also a multiple of p.

3. Using Euclid's Lemma and your choice of induction principle, prove the following lemma (without using the Fundamental Theorem of Arithmetic and *so on* kind of vague induction)

   Euclid's Lemma+. If a prime p divides a product of integers $a_1 a_2 \cdots a_k$, then p divides at least one of them. (2 points)

   - We will prove the lemma by induction on k. If $k = 1$, then the claim only says that if p divides a_1, then p divides a_1, which is trivially true.
   - Let $k > 1$ and the claim be true for $k - 1$. Let $b = a_2 \cdots a_k$.
   - Since p divides $a_1 b$, by Euclid's Lemma, p divides a_1 or b.

- If p, divides a_1, we are done.
- If p divides $b = a_2 \cdots a_k$, then p divides at least one of $a_2, \dots, a_k$.

4. Find as small a positive integer n as possible for which you can give a proof that the 100 consecutive numbers $n+1, n+2, \dots, n+100$ are all composite. Give a proof for your answer.

   Note: Any n with a correct proof will fetch you 2 points. But smaller n with proof will fetch more points. (4 points)

   - If you take $n = 101! + 1$, then $n + i = 101! + (i + 1)$ which is a multiple of $i + 1$ for all i in the range 1 to 100. Hence all those numbers are composite. (2 point answer)

   - If you take n as 1 more than the LCM of numbers 1 to 100, then also $n + i$ is a multiple of $i+1$ for all i in the range 1 to 100. Hence all those numbers are composite. (3 point answer)

   - If you take n as 1 more than the product of all prime numbers from 2 to 101, then $n + i$ is a multiple of each prime factor of $i + 1$ for all i in the range 1 to 100. Hence all those numbers are composite. (5 point answer)

5. A frog wants to climb a staircase with 10 steps. In a single forward jump it can cover either one or two steps. In how many different ways can the frog climb the staircase using forward jumps alone? (For example, if the staircase had only 3 steps, it can climb it in three different ways: $1 + 1 + 1$, $1 + 2$ or $2 + 1$.)

   Hint. Strong Induction. (4 points)

   Ans: 89. Let $f(n)$ denote the number of ways for the frog to climb a staircase with n steps as per the above rules.

   - $f(1) = 1$ since the only option is to make a single jump.
   - $f(2) = 2$ since we have the options: $1 + 1$ and 2
   - If there are n steps, $n \geq 2$, the first jump can be
     (a) a single step in which case there are $f(n-1)$ ways to complete the task, or
     (b) a double step in which case there are $f(n-2)$ ways to complete the task.
   - Hence $f(n) = f(n-1) + f(n-2)$. (Fibonacci numbers) (3 points)
   - Hence $f(10)$ is the the 10-th term in the Fibonacci sequence $1, 2, 3, 5, 8, 13, 21, 34, 55, 89$ which is 89. (1 point)

6. Truth tables of two propositional formulae α and β on propositional variables p, q, r are given below

p	q	r	α	β
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	T
F	T	T	T	T
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

   a) Write down a propositional formula in CNF and DNF for α and β directly from the truth table.

b) Simplify each one of them to a formula in which no variable repeats (6 points)

DNFs

$$
\begin{aligned}
\alpha = &(p \wedge q \wedge r) \\
&\vee (p \wedge q \wedge \neg r) \\
&\vee (p \wedge \neg q \wedge r) \\
&\vee (\neg p \wedge q \wedge r) \\
&\vee (\neg p \wedge q \wedge \neg r) \\
&\vee (\neg p \wedge \neg q \wedge r) \\
\beta = &(p \wedge q \wedge r) \\
&\vee (p \wedge q \wedge \neg r) \\
&\vee (p \wedge \neg q \wedge r) \\
&\vee (p \wedge \neg q \wedge \neg r) \\
&\vee (\neg p \wedge q \wedge r)
\end{aligned}
$$

CNFs

$$
\begin{aligned}
\alpha = &(\neg p \vee q \vee r) \\
&\wedge (p \vee q \vee r) \\
\beta = &(p \vee \neg q \vee r) \\
&\wedge (p \vee q \vee \neg r) \\
&\wedge (p \vee q \vee r)
\end{aligned}
$$

Simplified

$$
\begin{aligned}
\alpha &= q \vee r \\
\beta &= p \vee (q \wedge r)
\end{aligned}
$$