225 = 25·9 = 3²·5²
525 = 25·21 = 3·7·5²
∴ LCM = 3²·7·5² = 7·225 = 1575
GCF = 3·5² = 75

3 Typical questions:

3 | 93

1) Question: Which is a ~~prime number~~?

(a) ~~1002~~ (b) 101 (c) ~~93~~ (d) ~~187~~ 11 | 187

101 is prime, You only need to try numbers ≤ 10, since 11² > 101. 101 is odd, so you only need to try 3, 5, 7, 9.

2) Question: Which is the LCM of 225 and 525?

(a) 75 (b) 1575 (c) 105 (d) None of these

3) Question: Which is the GCF of 225 and 525?

(a) 75 (b) 1575 (c) 105 (d) None of these

or 525 = 225·2 + 75
225 = 75·3 + 0 ∴ 75

Note: If I ask you what the GCD or LCM of 2 numbers is, I don't care how you get the answer. However, there *will be* at least one problem which tests your ability to use the Euclidean Algorithm.

4) Question: Suppose M and N are relatively prime, that is, $\text{GCD}(M, N) = 1$. Which of the following is a true statement?

(a) there is no common multiple for M and N (b) $\exists r, s \in \mathbb{Z}\ (rM + sN = 1)$ (c) M or N is prime (d) All of these

(a) is always false (c) No, for example GCD(4,25) = 1

5) Question: Which of the following is *not* a consequence of the Fundamental Theorem of Arithmetic?

(a) Every integer greater than 1 has at least one prime factorization (b) Any two prime factorizations of an integer greater than 1 are the same except for the order of multiplication (c) There are infinitely many primes

This follows from Euclid's Thm

6) Question: What is the structure of a *proof by contradiction*?

(a) A sequence of statements, each of which is either a hypothesis, an axiom, or a logical consequence of earlier statements in the proof. (b) First assume that the conclusion is false, and derive from this a patently false statement. (c) Try many values of N, and then make a conjecture. (d) Find a counterexample, this proves that the theorem is false.

7) Question: What is the structure of a *direct proof*?

(a) A sequence of statements, each of which is either a hypothesis, an axiom, or a logical consequence of earlier statements in the proof. (b) First assume that the conclusion is false, and derive from this a patently false statement. (c) Try many values of N, and then make a conjecture. (d) Find a counterexample to prove that the theorem is false.

8) Question: To see if a large number N is prime, we check to see if $2, 3, 5, \ldots$ are factors. At what point can we stop and be sure that N is prime?

(a) Not until we've tried all primes less than N. (b) After we've tried all primes less than or equal to $N/2$ (c) After we've tried all primes less than or equal to $\sqrt{N}$

9) Question: What is the best translation for the statement $\forall M, N \in \mathbb{Z}^+ \; M|N$ and $N|M \implies M = N$?

(a) For any two positive integers, if each divides the other than they are the same. (b) There exist two positive integers, each of which divides the other and which are the same. (c) We select M and N so that each is a multiple of the other and they are the same. (d) If $M = N$ then M divides N and vice versa.

Last problems: You might get several problems like the next few, which ask you to identify the constituents of a theorem and proof. First, I will give you a statement and/or proof of a theorem, then follow it with some questions. (The theorem(s) on the exam will be different than this one.)

Theorem Let p be prime and a, b be positive integers, then there is an integer x such that "$as \equiv b \mod p$", that is, such that $p|(b - ax)$.

Proof: (I'll number the steps of the proof for later reference)

(i) Since p is prime, GCD(p, a)=1

(ii) Therefore, $\exists r, s \in \mathbb{Z}$ such that $pr + as = 1$

(iii) Then $pr = 1 - as$

(iii) Then $(pr)b = b - (as)b$

(iv) Put $x = sb$, then $p(rb) = b - ax$

(v) Then $p|(b - ax)$ (which is what we are trying to prove)$\square$

(The questions relating to this theorem and proof are on the next page)

10) Question: Which of the following is a *hypothesis* of this theorem?

(a) GCD(p, a)=1 (b) $p|(b - ax)$. (c) p is a prime (d) $\exists r, s \in \mathbb{Z}$ such that $pr + as = 1$

11) Question: Which of the following is a *conclusion* of this theorem?

(a) GCD(p, a)=1 (b) $p|(b - ax)$. (c) p is a prime (d) $\exists r, s \in \mathbb{Z}$ such that $pr + as = 1$

12) Question: Line (ii) of the proof...

(a) is a hypothesis; (b) Follows from line (1) by a lemma we proved in class; (c) follows from line (1) by fundamental rules of arithmetic; (d) follows from the definition of |

13) Question: Line (iii) of the proof...

(a) is a hypothesis; (b) Follows from earlier lines by a lemma we proved in class; (c) follows from earlier lines by fundamental rules of arithmetic; (d) follows from the definition of |

14) Question: Line (v) of the proof...

(a) is a hypothesis; (b) Follows from earlier lines by a lemma we proved in class; (c) follows from earlier lines by fundamental rules of arithmetic; (d) follows from the definition of |