

MATH 540: STUDY GUIDE AND PRACTICE PROBLEMS FOR EXAM I

The following is a list of topics and types of problems you should know for Exam I.

1. Be able to state the various theorems and definitions from class, and answer true-false type questions regarding them.
2. Mathematical Induction. Be able to apply mathematical induction to prove an elementary statement.
3. The Well Ordering Principle. Know how to state it and how to use it.
4. The Division Algorithm and its consequences. Be able to apply the division algorithm to find the GCD of two positive integers and use it to find the coefficients required in Bezout's principle. Similarly, be able to use Blankinship's method to write the GCD of A and b as an integer combination of A and b .
5. Know the relationship between the LCM and GCD of two positive integers.
7. Know the Fundamental Theorem of Arithmetic and its consequences, especially in regards to finding LCMs and GCDs.
8. Be able to verify that a given relation is an equivalence relation.
9. Know the formulas for $\tau(n)$, the number of divisors of n , and $\sigma(n)$, the sum of the divisors of n , and how to use them.
10. Know basic properties of and how to compute with integers modulo n , including solving simple linear equations.
11. Know the definition and properties of Euler's totient function.
12. Be able to work problems using Euler's theorem, Euler's product formula and Gauss's theorem.
13. Be able to work problems involving equivalence relations.
14. Be able to reproduce the proof of any one of the following three theorems:
 - (i) Every positive integer can be written as a product of prime numbers, i.e., the existence part of the Fundamental Theorem of Arithmetic.
 - (ii) If p is a prime number and $p|ab$, then $p|a$ or $p|b$.
 - (iii) Euler's Formula.

Practice Problems

1. Prove the following two statements by induction:
 - (a) $\sum_{k=1}^n (-1)^k k^2 = \frac{(-1)^n n(n+1)}{2}$.
 - (b) $\sum_{k=1}^n \frac{1}{k(k+1)} = \frac{n}{n+1}$.
2. Let $d_1 = \frac{2}{3}$ and $d_2 = \frac{3}{5}$. For $n \geq 3$, set $d_n := d_{n-1} \cdot d_{n-2}$. Use the Well Ordering Principle to show that $d_n < 1$, for all $n \geq 1$.
3. Use Let $a = \sigma(24)$ and $b = \tau(24)$. Here $\sigma(24)$ means the sum of the divisors of 24 and $\tau(24)$ means the number of divisors of 24. Use the division algorithm to find $\text{GCD}(a, b)$. Then use Bezout's Principle to write $\text{GCD}(a, b)$ as a combination of a and b . Finally, find $\text{LCM}(a, b)$.

4. Use the Fundamental Theorem of arithmetic to find the GCD and LCM of 63,000 and 36,690.
5. Consider the relation on $\mathbb{Z}^+ \times \mathbb{Z}^+$ given by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$.
 - (a) Prove that \sim is an equivalence relation.
 - (b) Describe the equivalence class of $(3, 5)$.
 - (c) Let X be the set of equivalence classes of \sim . Define $f : X \rightarrow \mathbb{Z}$, by $f([(a, b)]) = a - b$. Prove that f is well defined, in other words, the value of f does not change if we use a different representative for the class $[(a, b)]$.
6. For $n \geq 2$, let \mathbb{Z}_n denote the integers modulo n .
 - (a) Write out addition and multiplication tables for \mathbb{Z}_7 .
 - (b) Can you explain why every non-zero element of \mathbb{Z}_7 has a multiplicative inverse?
 - (c) Find a solution to the congruence $7x \equiv 5 \pmod{12}$.
 - (d) Find an integer n so that the congruence $7x \equiv 5 \pmod{n}$ does *not* have a solution.
 - (e) Find all solutions to $12x \equiv 15 \pmod{21}$, both in \mathbb{Z}_{21} and in \mathbb{Z} .
 - (f) Find all solutions to the equation $x^2 - 1 \equiv 0 \pmod{35}$.
7. Find the multiplicative inverse of 27 modulo each of 31, 33, 34. Hint: Euler's theorem might be useful.
8. Find $139^{112} \pmod{27}$.
9. Find $\phi(1492), \phi(1776), \phi(2001)$.
10. Find all positive integers n such that $\frac{\phi(n)}{n} = \frac{1}{2}$.