

# Math 287 Fall 2024, Sample Test II

Randall Holmes

November 13, 2024

This is probably a bit longer than the actual test (not much longer). I will take questions about it on Thursday, and Ill post solutions on Sunday or Monday.

The actual test will have some selected definitions and theorems on it, but you really should be suere to be familiar with any concepts used here.

1. (paired with 2) Prove using the recursive definition of summation and mathematical induction that  $\sum_{i=1}^n (x_i + y_i) = \sum_{i=1}^n x_i + \sum_{i=1}^n y_i$ .

2. (paired with 1) Prove using the recursive definition of summation and mathematical induction that  $\sum_{i=a+r}^{b+r} a_i = \sum_{i=a}^b a_{i+r}$ .

3. (paired with 4) Give a Venn diagram demonstration of the identity  $A - (B \cup C) = (A - B) \cap (A - C)$ . You need to draw a diagram for each side of the equation, with appropriate shadings of sets used in the calculation, and clearly outline the result set in each diagram so a reader can see that they are the same.

4. (paired with 3) State the recursive definitions of  $\bigcap_{i=a}^b A_i$  and  $\bigcup_{i=a}^b A_i$ .  
Prove by mathematical induction that  $A - \bigcap_{i=1}^n A_i = \bigcup_{i=1}^n (A - B_i)$

5. (paired with 6) Using the extended Euclidean algorithm theorem, prove Euclid's Lemma: if  $p$  is a prime and  $p|ab$ , then either  $p|a$  or  $p|b$ .

6. (paired with 5) Make an addition and a multiplication table for mod arithmetic, and a table of additive inverses, and a table of multiplication inverses.

Prove that for any modulus  $m$ , if  $a \equiv_m c$  and  $b \equiv_m d$ , then  $ab \equiv_m cd$ .

7. (unpaired) Prove by strong induction that each integer  $\geq 2$  is a prime or a finite product of primes.

Another theorem which might appear here is that there are infinitely many primes.

8. Multiplicative inverses in modular arithmetic

- (a) Prove that for each prime  $p$  and for each  $a$  with  $0 < a < p$  there is a unique  $b$  with  $0 < b < p$  such that  $ab \equiv_p 1$ . Hint: use the extended Euclidean algorithm theorem.
- (b) Find integers  $x$  and  $y$  such that  $211x + 34y = \gcd(211, 34)$ . Show all calculations.
- (c) Find the multiplicative inverse of 34 in mod 211 arithmetic. Your answer should be a remainder mod 211.
- (d) Solve the equation  $34x \equiv_{211} 55$ . Your answer should be a remainder mod 211.



9. Chinese remainder theorem

Solve the system of equations

$$x \equiv_{37} 2$$

$$x \equiv_{101} 9$$

State the smallest positive solution. State another solution. State the general form of the solution (describing all integers which are solutions).

10. Modular exponentiation

- (a) Compute  $37^{55} \bmod 100$  by the method of repeated squaring.
- (b) Compute  $21^{75} \bmod 37$ . Hint: Fermat's little theorem might be useful.