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 $\sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$.

Basis: $\sum_{i=1}^{1}(x_i + y_i) = x_1 + y_1 = \sum_{i=1}^{1} x_i + \sum_{i=1}^{1} y_i$

Let $k \in \mathbb{N}$ be chosen arbitrarily

Induction Hyp: $\sum_{i=1}^{k}(x_i + y_i) = \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i$

Goal: $\sum_{i=1}^{k+1}(x_i + y_i) = \sum_{i=1}^{k+1} x_i + \sum_{i=1}^{k+1} y_i$

Proof: $\sum_{i=1}^{k+1}(x_i + y_i) \overset{\text{def } \Sigma}{=} \left(\sum_{i=1}^{k} x_i + y_i\right) + x_{k+1} + y_{k+1}$

$\overset{\text{ind hyp}}{=} \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i + x_{k+1} + y_{k+1}$

$\overset{\text{alg}}{=} \left(\left(\sum_{i=1}^{k} x_i\right) + x_{k+1}\right) + \left(\sum_{i=1}^{k} y_i\right) + y_{k+1}$

$= \sum_{i=1}^{k+1} x_i + \sum_{i=1}^{k+1} y_i$

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

Basis: $\sum_{i=a+r}^{a+r} a_i = a_{a+r} = \sum_{i=a}^{a} a_{i+r}$ ✓

Induction Let $k \in \mathbb{N}$ be chosen arbitrarily

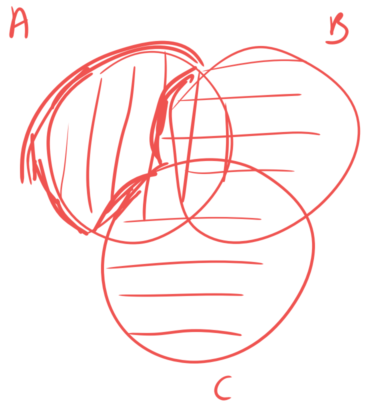
Suppose that $\sum_{i=a+r}^{k+r} a_i = \sum_{i=a}^{k} a_{i+r}$

Goal: $\sum_{i=a+r}^{(k+1)+r} a_i = \sum_{i=a}^{k+1} a_{i+r}$

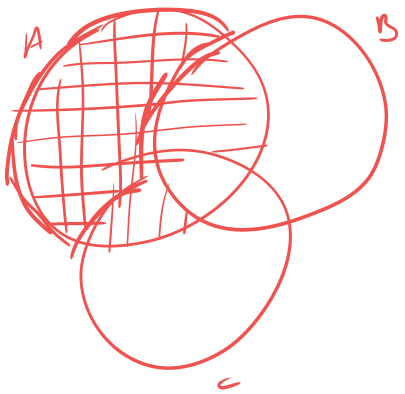
Proof: $\sum_{i=a+r}^{(k+1)+r} a_i = \sum_{i=a+r}^{(k+r)+1} a_i \overset{\text{def } \Sigma}{=} \sum_{i=a+r}^{k+r} a_i + a_{(k+r)+1}$

$\overset{\text{ind hyp}}{=} \sum_{i=a}^{k} a_{i+r} + a_{(k+1)+r} = \sum_{i=1}^{k+1} a_{i+r}$ ✓

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.



A |||| $B \cup C$ ≡



A - B ||| A - C ≡

outlined sets 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 $A - \bigcap_{i=1}^{n} A_i = \bigcup_{i=1}^{n}(A - B_i)$

B typo

$$\bigcap_{i=a}^{a} A_i = A_a \qquad \bigcap_{i=a}^{n+1} A_i = \left(\bigcap_{i=a}^{n} A_i\right) \cap A_{n+1}$$

$$\bigcup_{i=a}^{a} A_i = A_a \qquad \bigcup_{i=a}^{n+1} A_i = \left(\bigcup_{i=a}^{n} A_i\right) \cup A_{n+1}$$

Basis: $A - \bigcap_{i=1}^{1} B_i = A - \underline{B_1} = \bigcup_{i=1}^{1} A - B_i$

Induction Suppose it holds for $k \in \mathbb{N}$:

$$A - \bigcap_{i=1}^{k} B_i = \bigcup_{i=1}^{k} (A - B_i)$$

Then $A - \bigcap_{i=1}^{k+1} B_i = A - \left(\bigcap_{i=1}^{k} B_i \cap B_{k+1}\right) =$ (other deM law)

$\left(A - \bigcap_{i=1}^{k} B_i\right) \cup A - B_{k+1} =$ (ind hyp)

$\bigcup_{i=1}^{k} (A - B_i) \cup (A - B_{k+1}) =$ (def $\cup$)

$\bigcup_{i=1}^{k+1} (A - B_i)$

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 $p|b$.

Suppose p is prime and $p|ab$.

If $p|a$ then $p|a \vee p|b$.

If $p \nmid a$ then $\gcd(p,a)=1$ so $\exists u,v$ s.t. $pu+av=1$

$b = b \cdot 1 = b(pu+av) = bpu + bav$ is divisible by p.

divisible by p

divisible by p because $p|ab$

6. (paired with 5) Make an addition and a multiplication table for mod 7 arithmetic, and a table of additive inverses, and a table of multiplication inverses.

annoying typo!

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

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	0	1	2	3
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

n	$-n$
0	0
1	6
2	5
3	4
4	3
5	2
6	1

n	n^{-1}
0	—
1	1
2	4
3	5
4	2
5	3
6	6

Suppose $a \equiv_m c$ and $b \equiv_m d$. Then $a = c + mk$, $b = d + m\ell$ for some $k, \ell \in \mathbb{Z}$

So $ab = (c+mk)(d+m\ell) = cd + mkd + cm\ell + mkm\ell$
$= cd + m(kd + c\ell + mk\ell)$
$\equiv_m ab$ ✓

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

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

   Both theorem are in the notes.

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 $211x + 34y = \texttt{gcd}(211, 34)$. 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.

a: Suppose p is prime, $0<a<p$. Then $\gcd(p,a)=1$,

$\exists u,v$ $pu + av = 1$ so $av \equiv_p 1$ and $a(v \bmod p) \equiv_p 1$

while $0 < v \bmod p < p$ - let $b = v \bmod p$.

Suppose it wasn't unique: if $ab \equiv_p 1$ and $ac \equiv_p 1$ and

$0<b<c<p$ then $a(c-b) = ac - ab \equiv_p 1-1 = 0$

but $0 < c-b < p$ so this is impossible because

p is prime.

b.

211	1	0	
34	0	1	
7	1	-6	6
6	-4	25	4
1	5	-31	1

so $5 \cdot 211 - 31 \cdot 34 = 1 = \gcd(211, 34)$

c. $(-31) \cdot 34 \equiv_{211} 1$ so $211 - 31 = \boxed{180}$ is the inverse.

d. $34x \equiv_{211} 55$

$x \equiv_{211} 55 \cdot 180 \equiv_{211}$

$9900 - 46 \cdot 211 = \boxed{194}$

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).

$x = 9 + 101k$

$9 + 101k \equiv_{37} 2$

$101k \equiv_{37} \cancel{2} - 9 + 37 = 30$

$101 - 2(37) = 27$

$27k \equiv_{37} 30$

find 27^{-1} mod 37 is 11

37	1	0
27	0	1
10	1	-1
7	-2	3
3	3	-4
1	-8	11

$k \equiv_{37} 30 \cdot 11 \equiv_{37} 330 - 8 \cdot 37 = 34$

$x = 9 + 101k = 9 + (101)(34) = \boxed{3443}$

mod $37 \cdot 101 = 3737$, 3443 is smallest, 7180 is another, $3443 + k \cdot 3737$ is general

10. Modular exponentiation

(a) Compute $37^{55}\texttt{mod}100$ by the method of repeated squaring.

(b) Compute $21^{75}\texttt{mod}37$. Hint: Fermat's little theorem might be useful.

a.

55	$33^2 \cdot 37 \bmod 100 = \boxed{93}$
27	$97^2 \cdot 37 \bmod 100 = 33$
13	$9^2 \cdot 37 \bmod 100 = 97$
6	$53^2 \bmod 100 = 9$
3	$37^2 \cdot 37 \bmod 100 = 53$
1	$37^1 = 37$

b. $21^{95} \bmod 37 = 21^{75 \bmod 36} \bmod 37$ by FLT

$= 21^3 \bmod 37 = 9261 - (250)(37) = \boxed{11}$