Math 3336 : Test 2 Review

Instructions

- This is not an assignment. Neither work nor answers are to be submitted.
- Also, **DON'T FORGET THAT** $0 \in \mathbb{N}$.

---

1. How many...

(a) binary strings of length 300 begin with 01 and end with 111?

$0\,1\,\underbrace{\_\,\_\,\_\,\cdots\,\_\,\_\,\_}_{295}\,1\,1\,1$

$\boxed{2^{295}}$

(b) binary strings of length 300 contain an even number of 0s?

$\boxed{2^{299}}$

(c) subsets of $X = \{A, B, C, D, E\}$ have cardinality equal to 2? 3?

Cardinality 2

$\binom{5}{2} = \frac{5!}{3! \cdot 2!} = \boxed{10}$

Cardinality 3

$\binom{5}{3} = \frac{5!}{2!\,3!} = \boxed{10}$

(d) length-12 lists (made from the symbols $\{A, B, C, D, E, F, G, H, I, J, K, L\}$) are there? How many contain the word $BACK$?

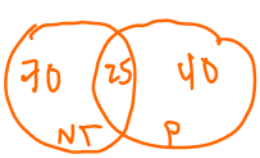
12 symbols

$\boxed{\#\text{ length 12 lists} = 12!}$

$\boxed{\#\text{ containing "BACK"} = 9 \cdot 12^8}$

---

2. A math test contains 150 questions, 70 of which are about Number Theory, 40 of which are about Proofs, and 25 of which are about both Number Theory and Proofs. How many questions are *exclusively* about Number Theory? How many questions are there that do not ask about either Number Theory or Proofs?



\# only number theory

$= 70 - 25 = \boxed{45}$

\# neither NT nor Proofs

$150 - 70 - 40 + 25$

$= \boxed{65}$

3. Write a proof by induction that for every $n \in \mathbb{N}$ the sum of the first n consecutive natural numbers equals $\binom{n+1}{2}$

Recall: $\binom{n+1}{2} = \frac{(n+1)!}{2! \cdot (n-1)!} = \frac{(n+1) \cdot n \cdot (n-1)!}{2 \cdot (n-1)!} = \frac{(n+1)n}{2}$

Base Case $n = 0$

$$\sum_{i=0}^{n} i = 0 = \frac{(0+1)0}{2} \checkmark$$

Inductive Step Suppose $\sum_{i=0}^{k} i = \frac{(k+1) \cdot k}{2}$ for some $k \in \mathbb{N}$.

(We WTS $\sum_{i=0}^{k+1} i = \frac{(k+2)(k+1)}{2}$)

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + k+1 = \frac{(k+1)k}{2} + k+1$$

$$= \frac{(k+1)k}{2} + \frac{2(k+1)}{2} = \frac{(k+1)k + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

Where we used our ind. hyp. after the second equal sign

4. Consider the set $S \subseteq \mathbb{Z}$ that is recursively defined by the following rules:

$$9, 15 \in S$$
$$x, y \in S \Rightarrow ax + by \in S \text{ (for all integers } a, b \in \mathbb{Z})$$

Explore the set S. For instance, find four different integers that are in S. Notice how each one is a multiple of 3? Write or outline a proof by Structural Induction that *all* elements of S are multiples of 3.

$9 + 15 = 24 \in S$ $\quad 18 - 15 = 3 \in S$ $\quad -9 + 30 = 21 \in S$

$0 + 0 = 0 \in S$

Base Case

9 + 15 are mult. of 3

Recursive Step

$x, y \in S$ are mult.'s of 3 + $u, v \in \mathbb{Z}$,

then $xu + yv = 3mu + 3nv = 3(mu + nv)$

for some $m, n \in \mathbb{Z}$. Therefore $xu + yv$ is a mult. of 3 for all $u, v \in \mathbb{Z}$.

5. Write down the following amazing items:

(a) The Division "Algorithm"

$\forall\ a,b \in \mathbb{Z},\ \exists!\ q,r \in \mathbb{Z}.\quad a = qb + r$

and $\quad 0 \leq r < |b|$

(b) Euclid's Lemma

$\forall\ a,b,p \in \mathbb{Z},$ if p is prime and $p \mid (ab)$

then $p \mid a \vee p \mid b$.

(c) Bezout's Identity

$\forall\ a,b \in \mathbb{Z},\ \exists\ x,y \in \mathbb{Z},\quad ax + by = \gcd(a,b)$

(d) The Fundamental Theorem of Arithmetic

$\forall\ a \in \mathbb{Z},\ a > 1,\quad a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where p_i are primes

(e) The meaning / definition of the statement "a and b are relatively prime."

$\gcd(a,b) = 1$

(f) The meaning / definition of "$a \equiv b \bmod n$"

$a - b = k \cdot n$ for some $k \in \mathbb{Z}$

OR $\quad a$ & b have same remainder when divided by n.

6. Solve the recurrence equation

$$a_n = 3a_{n-1} + 10a_{n-2}$$

with initial conditions $a_0 = 2$ and $a_1 = 8$.

char. equation: $x^2 - 3x - 10 = (x-5)(x+2)$

roots: $r_1 = 5$, $r_2 = -2$

$a_n = \alpha \cdot 5^n + \beta \cdot (-2)^n$

$n=0$: $2 = \alpha + \beta$

$n=1$: $8 = 5\alpha - 2\beta$

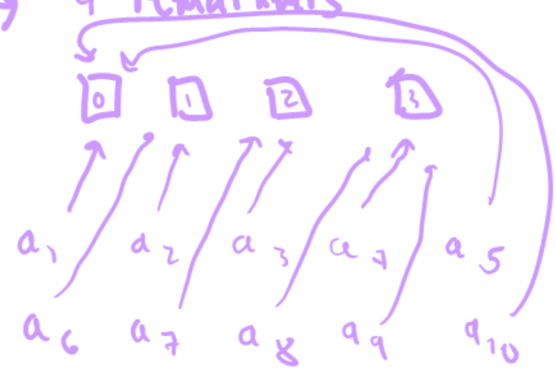
$\longrightarrow$ $\alpha = \frac{12}{7}$, $\beta = \frac{2}{7}$

$\longrightarrow$ $\boxed{a_n = \frac{12}{7} 5^n + \frac{2}{7}(-2)^n}$

---

7. 10 integers are selected at random, and they are each divided by a positive natural number, n. Moreover, we are also told that *at least* 3 of these remainders are equal. What is the largest possible value of n? How do you know?

$n = 4$ $\longrightarrow$ 4 remainders



if $n = 5$, then we only know 2 or more for sure

---

8. Use the Euclidean Algorithm to compute the gcd(2022, 1455).

$2022 = 1 \cdot 1455 + 567$

$1455 = 2 \cdot 567 + 321$

$567 = 1 \cdot 321 + 246$

$321 = 1 \cdot 246 + 75$

$246 = 3 \cdot 75 + 21$

$75 = 3 \cdot 21 + 12$

$21 = 1 \cdot 12 + 9$

$12 = 1 \cdot 9 + 3$

$9 = 3 \cdot 3 + \boxed{0}$

$\gcd(2022, 1455) = 3$

9. Write a proof that for all integers $a, b \in \mathbb{Z}$

$$\Big(\gcd(a,b) = a\Big) \iff \Big(b \equiv 0 \bmod a\Big).$$

(We may assume $a > 0$.)

$(\Rightarrow)$

$\gcd(a,b) = a$ means

$a \mid b \Rightarrow b = m \cdot a$

$\Rightarrow b \equiv 0 \bmod a$

$(\Leftarrow)$ $b \equiv 0 \bmod a$

$\Rightarrow b = m \cdot a$

since $a = \max D_+(a)$,

it follows that $a = \gcd(a, ma)$.

10. Consider the congruence equation $12x \equiv b \bmod 8$.

(a) Are there any values we can use for b so that the congruence equation has no solutions? If so, provide one and explain why it works. If not, explain why.

$b = 5$

$\gcd(12, 8) = 4$ and $4 \nmid 5$

(b) Are there any values we can use for b so that the congruence equation has only one solution in the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$? If so, provide one and explain why it works. If not, explain why.

no, $\gcd(12, 8) \neq 1$

(c) Are there any values we can use for b so that the congruence equation has more than one solution in the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$? If so, provide one and explain why it works. If not, explain why.

yes, $b = 4$ $\gcd(12, 8) \mid 4$ and $\gcd(12, 8) > 1$

so mult. solutions in $\{0, 1, 2, 3, 4, 5, 6, 7\}$

(d) Are there any values we can use for b so that the congruence equation has more than one integer solution but less than 10? If so, provide one and explain why it works. If not, explain why.

no, if there are solutions then there will be infinitely many in $\mathbb{Z}$ (add mult.'s of 8)

11. Find all solutions to the congruence equation

$$24x \equiv 32 \bmod 64$$

Which of these solutions are in the set $\{0, 1, 2, \cdots, 62, 63\}$?

$\gcd(24, 64) = 8 \quad 8 \mid 32 \ \checkmark$

reduce equation $\longrightarrow \quad 3x \equiv 4 \bmod 8$

$3 \cdot 3 \equiv 1 \bmod 8$ so $3^{-1} = 3 \longrightarrow \quad x \equiv 12 \bmod 8 \equiv 4 \bmod 8$

$x_0 = 4$ also have $4+8 = 12, \ 20, \ 28, \ 36, \ 44, \ 52, \ 60$

solutions (in set) $\rightarrow \boxed{4, 12, 20, 28, 36, 44, 52, 60}$

12. Write a proof (by induction) of the following:

Proposition. The sum of the first n odd numbers equals n^2

<u>Base Case $n=1$</u>

$1 = 1^2 \ \checkmark$

<u>Ind Step</u>

Suppose $\sum_{i=1}^{k} (2i-1) = k^2$. $\quad \sum_{i=1}^{k+1} (2i-1) = \sum_{i=1}^{k} (2i-1) + 2k+1$

$= k^2 + 2k + 1 = (k+1)^2$, where ind hyp. was used after second = sign.

13. Consider the recursively-defined set $S \subseteq \mathbb{Z} \times \mathbb{Z}$:

$$(1,1), (-1,-1) \in S$$
$$(x,y), (a,b) \in S \Rightarrow (x+a, y+b) \in S$$

Use Structural Induction to prove that if $(x,y) \in S$ then $x = y$.

<u>Base Case</u>

(1,1) satisfies $x = 1 = y$

(-1,-1) satisfies $x = -1 = y$

<u>Recursive Step</u>

Suppose $(x,y), (a,b) \in S$ satisfy $x = y$ & $a = b$.

Then $(x+a, y+b) = (x+a, x+a)$ and so have 2nd & 1st components equal $\square$