Ma2201/CS2022 Final Exam.

Discrete Mathematics

a Term, 2017

Print Name: ____________________

Sign: ____________________

Do any **six** of the following eight problems:

1. (**5 pts**) Prove by induction that

$$1 + 4\sum_{k=0}^{n} 5^k = 5^{n+1}$$

for all $n \geq 0$.

Your proof must be clear, neat, and complete. You may use 'strong induction.' You may also prove more than is asked.

♣ Proof. The Base Case, n=0. Here the sum has only one term, and we compute $1 + 4\frac{1}{5^0} = 1 + 4 = 5 = 5^{0+1}$, as required.

Let the equation be true for some particular n: $1 + 4\sum_{k=0}^{n} 5^k = 5^{n+1}$. Now we compute

$$\begin{aligned} 1 + 4\sum_{k=0}^{n+1} 5^k &= \left[1 + 4\sum_{k=0}^{n} 5^k\right] + 4 \cdot 5^{n+1} \quad \text{split off the last term} \\ &= 5^{n+1} + 4 \cdot 5^{n+1} \quad \text{By the induction hypothesis} \\ &= 5^{n+1}(1+4) = 5^{n+2} = 5^{(n+1)+1} \end{aligned}$$

as required.

Since the statement is true for the base case $n = 0$, and the induction step is true for all n, the statement is true for all $n \geq 0$ by induction. ♠

2. (**5 pts**) Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

a) How many sets are subsets of A?

♣ $2^{|D|} = 2^{10}$. ♠

b) How many subsets of A are also subsets of a subset of A? ♣ $A \subset A$, so 2^{10} again.

♠

c) How many subsets of A do not contain an element of $B = \{0, 2, 3, 4, 9\}$ ♣ ♠

Multiplicative principle says 2^5.

d) What is the 666'th element of $A \times A \times A$ is lexicographic order. ♣ There are 10

possibilities in each coordinate, so using division with remainder:

$666 = 66 \cdot 10 + 6$, so the last coordinate is the 6'th element, counting from 0, so 6.

$66 = 6 \cdot 10 + 6$, so the middle coordinate is the 6'th element of D, counting from 0, so 6 again, and lastly

$6 = 0 \cdot 10 + 6$, so the first coordinate is the 6'th element of D, counting from 0, so 6 again.

Therefore $(6, 6, 6) \ldots$ oh $\ldots$ of course! ♠

3. (**5 pts**) Let A, B and C be sets with $|A| = 5$ and $|B| = 24$ and $|C| < |A|$ Label each of the following as **TRUE** if true, or **FALSE** if false and **?** if it cannot be determined from the given information.

____ $\emptyset \in A \cap C$.

♣ **?**: The empty set is a subset of every set, but without knowing A or C, we cannot tell $\emptyset$ is an element of the set. ♠.

____ $B = \mathcal{P}(A \cap C)$.

♣ **F**: If B were a powerset of a finite set, its cardinality would have to be a power of 2, and not 24. ♠

____ There is a one-to-one function from $\mathcal{P}(C)$ into $\mathcal{P}(A \cup B)$.

♣ **T**: $|C| \leq |A| \leq |A \cup B|$, so a one to one function exists. ♠

____ There is a one-to-one and onto function from B into $\mathcal{P}(A \cap B \cap C)$.

♣ **F**: Deja Vu. If B had the cardinality of the powerset of a finite set, its cardinality would have to be a power of 2, and not 24. ♠

____ There are 29! onto functions from $A \times B$ into $B \times A$.

♣ **F**: The cardinality of the two sets is equal, so the number of onto functions equals the number of one-to-one functions, and is a factorial, but $|A \times B| = |B \times A| = 5 \cdot 24 = 120$, not 29. So there are 120! onto functions. ♠

4. (**5 pts**) Let p, q, and r be statements.

a) Write the expression $((p \Rightarrow \neg q)) \Rightarrow r$ using only p, q, r,), (, $\wedge$, $\vee$, and $\neg$, and with $\neg$ outside of no parenthesis.

♣ You can use the definition of $\Rightarrow$ first to remove that symbol: $[(p \Rightarrow \neg q) \Rightarrow r] = \neg(p \Rightarrow \neg q)) \vee r = \neg(\neg p \vee \neg q) \vee r$.

Now the $\neg$ outside the parenthesis can be moved inside with Demorgan's law: $\neg(\neg p \vee \neg q) \vee r = (p \wedge q) \vee r$ which satisfies the requirements. and by the distributive law so does $(p \vee r) \wedge (q \vee r)$. ♠

b) Find any truth values for p, q, and r which make the expression in part a TRUE.

♣ From the original expression, if r is true, the implication is true, in which case the values of p and q do not matter, so $p = TRUE$, $q = TRUE$ and $r = TRUE$ works just fine. ♠

5. (**5 pts**) Let $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
a) How many relations are there on the set D which are reflexive?

♣ Reflexive means that the 10 elements of the form (k, k) must be in the relation. So there is no choice there. Otherwise, relation is just a subset of $D \times D$, and $|D \times D| = 10^2 = 100$, so for each of the $100 - 10$ elements of $D \times D$, we can choose whether or not it is the relation. So there are 2^{90} reflexive relations. ♠

b) How many relations are there on the set D which are both reflexive and symmetric.

♣ Reflexive means that the elements (k, k) must be in the relation for all $k \in D$. So there is no choice there.

Symmetric means that if (j, k) is in the relation so is (k, j). So the relation is determined by which pairs of distinct elements are related to one another. So from the calculation above, half of the choices are removed, so $2^{90/2} = 2^{45}$.

Alternatively, the set of such pairs is the set of subsets of D of cardinality 2, that is $\mathcal{P}_2(D)$, and they can be independently chosen, so there are $2^{|\mathcal{P}_2(D)|} = 2^{\binom{10}{2}} = 2^{10!/((2!)(8!))} = 2^{10\cdot 9/2} = 2^{45}$ relations. ♠

6. (**5 pts**) Find **all** values $x \in \mathbb{Z}$ which satisfy both of the conditions $x \equiv 72 \bmod 101$ and $x \equiv 7 \bmod 11$. Your answer can be in the form of an algebraic expression.

♣ A solution is guaranteed by the Chinese Remainder Theorem since $\gcd(11, 101) = 1$. We start with the Euclidean algorithm:

$$\begin{array}{rrcl} -5: & 101 & = & 9 \cdot 11 + 2 \\ 1: & 11 & = & 5 \cdot 2 + 1 \end{array}$$

so $(-5)(101) + (46)(11) = 1$. So $(7)(-5)(101) + (72)(46)(11)$ is a solution.

Now, to find all solutions you take: $x = (7)(-5)(101) + (72)(46)(11) + k(11)(101)$ for all $k \in \mathbb{Z}$.

If you did the extra arithmetic you might have gotten $x = 1789 + k1111$. ♠

7. (**5 pts**) a) Find the multiplicative inverse of 59 modulo 129.

♣ To find the multiplicative inverse of 59 modulo 129. We use the Euclidean Algorithm:

$$\begin{array}{rrcl} -16: & 129 & = & 2\cdot 59+11 \\ 3: & 59 & = & 5\cdot 11+4 \\ -1: & 11 & = & 2\cdot 4+3 \\ 1: & 4 & = & 1\cdot 3+1 \end{array}$$

so $(-16)(129)+(35)(59)=1$, so the multiplicative inverse is 35. ♠

b) Solve $59x \equiv 10 \bmod 129$

♣ Multiplying both sides by the multiplicative inverse of 59 we get $(35)(59)x \equiv (35)10 \bmod 129$, so that $x \equiv 350 \bmod 129$.

So $x \equiv 350 \bmod 129$ is a correct answer. If you want to express it as a value between 0 and 128, you divide 350 by 129 and get remainder 92, so $x \equiv 92 \bmod 129$ is also correct. ♠

8. (**5 pts**) Suppose that p, q, are r are primes, with $2 < p < q < r$.

Label each of the following **TRUE** if it must be true, **FALSE** if it must be false and **HUH?** if not enough information is given.

(Be careful, to get full credit you must distinguish between **FALSE** and **HUH?**.)

____ $p^2 - q^2$ is not prime.

TRUE: You could argue, p and q are two primes larger than 2, so they are both odd, so p^2-q^2 is even, and larger than 2, so not prime. Or you could factor it: $p^2-q^2=(p+q)(p-q)$, and $p-q \neq 1$, or other arguments.

____ $\gcd(p^3q, pq^5) > q$.

TRUE: Since we have the prime factorizations, $\gcd(p^3q, pq^5) = pq$ which is larger than q.

____ The number $p^2q^3r^5 + p^3q^5r^2 + p^5q^2r^3$ is not prime.

TRUE: $p^2q^2r^2 \mid p^2q^3r^5 + p^3q^5r^2 + p^5q^2r^3$ so it is not prime.

____ Dividing r by q leaves remainder p.

HUH?: Since $p < q$, it is possible, but not certain. For instance primes 3, 7 and 17 works, but 11, 13, and 19 do not.

____ $3 \mid q^3r^{33}$.

FALSE: Neither q nor r is 3 since they are too large, and q^3r^{33} is the unique prime factorization of that number.