Exam 2 – Math 215

Problem 1 (35 points; 5 points each). Decide if each of the following are true or false. You do not need to justify your choice here.

(a) <u>TRUE</u> $13x + 9 \equiv -x + 2 \pmod{7}$ for all x.

This is true since $13 \equiv 6 \equiv -1 \pmod{7}$ and $9 \equiv 2 \pmod{7}$.

(b) <u>FALSE</u> It is possible for a to have an inverse modulo b while b fails to have an inverse modulo a.

This is false since a has an inverse modulo b iff $\gcd(a, b) = 1$.

(c) <u>TRUE</u> If $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$ where p and q are distinct primes, then $x \equiv a \cdot b \pmod{p \cdot q}$.

This is a consequence of the Chinese Remainder Theorem.

(d) <u>TRUE</u> If $n + 1$ distinct integers are taken from the integers $1, 2, \ldots, 2n$, then at least one pair of consecutive integers must be chosen.

This is a simple application of the pigeon hole property.

(e) <u>TRUE</u> $G(X) = (1 + x)^n$ is a generating function for $a_m = \binom{n}{m}$.

This is the binomial theorem, binomial expansion.

(f) <u>FALSE</u> $a_n = 3 \cdot a_{n-1} + 2 \cdot a_{n-3}$ is a linear, homogeneous, 2^{nd}-degree recurrence relation.

This is 3^{rd}-degree, not 2^{nd}-degree.

(g) <u>TRUE</u> If $f(n)$ and $g(n)$ are solutions to $a_n = 3a_n - 2a_{n-1} + a_{n-3}$, then $c_1 \cdot f(n) + c_2 \cdot g(n)$ where c_1 and c_2 are scalars (real or complex), is also a solution.

Linear combinations of solutions are solutions.

Problem 2 (Multiple Choice; 35 points; 5 points each). You may select any number of choices, 0 – 4. You get one point per each correct item, meaning if the item should be selected you get a point, if it should not be selected you get a point.

(a) Which of the following hold?

$\otimes$ $a + b \equiv (a \mod n) + (b \mod n) \pmod n$
$\otimes$ $a \cdot b \equiv (a \mod n) \cdot (b \mod n) \pmod n$
$\bigcirc$ $a^b \equiv (a \mod n)^{(b \mod n)} \pmod n$
$\otimes$ $b - a \equiv (b \mod n) - (a \mod n) \pmod n$.

(b) Which of the following are equivalent to $\gcd(a, b) = 1$?

$\otimes$ a and b are relatively prime.
$\otimes$ There are integers s and t so that $sa + tb = 1$.
$\otimes$ $ax \equiv 1 \pmod b$ has a solution.
$\otimes$ $ax \equiv c \pmod b$ has a solution for all c.

(c) Which of the following have solutions?

$\bigcirc$ $x^2 \equiv 5 \pmod 7$.
$\bigcirc$ $x^2 \equiv 7 \pmod 5$.
$\bigcirc$ $x^2 \equiv 7 \pmod{11}$.
$\otimes$ $x^2 \equiv 11 \pmod 7$.

(d) What is the largest number required to compute $999^{2001} \mod 500$ using the "fast exponentiation" algorithm that we studied?

$\bigcirc$ 500^2
$\bigcirc$ 1001^2.
$\otimes$ 499^2.
$\otimes$ 499. (Either or both of these)

(e) Which of the following equations hold?

$\otimes$ $4^n = \sum_{i=0}^{2n} \binom{2n}{i}$
$\otimes$ $4^n = \sum_{i=0}^{n} \binom{n}{i} 2^n$
$\otimes$ $4^n = \sum_{i=0}^{n} \binom{n}{i} 3^i$
$\otimes$ $4^n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} 5^i$.

(f) How many distinct strings of length 5 can be made from the 26 lowercase letters a, b, c, ..., z if letters are allowed to repeat.

⊗ 26^5.
○ 5^{26}.
⊗ The number of ways of distributing 5 labeled balls into 26 labeled bins.

$$\sum_{\substack{n_i \in \mathbb{Z}^+ \\ n_1+n_2+\cdots+n_{26}=5}} \frac{5!}{n_1! \cdot n_2! \cdots n_{26}!}$$

○ The number of ways of distributing 5 labeled balls into 26 labeled bins.

$$\sum_{\substack{n_i \in \mathbb{Z}^+ \\ n_1+n_2+\cdots+n_5=26}} \frac{26!}{n_1! \cdot n_2! \cdots n_5!}$$

(g) How many 8 bit strings either start with 10 or end with 10?

○ $2^6 + 2^6$.
○ $2^8 - 2^4$.
⊗ $2^6 + 2^6 - 2^4$.
⊗ $2^7 - 2^4$.

Problem 3 (Computation; 60 points; 15 points each)**.** Choose **four** of the five problems, I will grade the first four chosen, so if you do all five and get 1, 2, 3, and 5 correct but 4 wrong, you will score 30/40, since I will have graded 1 - 4. It is your job to decide which four I grade.

(a) Use Fermat's Little Theorem to compute $900^{900} \mod 19$.

This is trivial, 19 is prime so $900^{18} \equiv 1 \pmod 19$ if $19 \not| 900$. But $900/18 = 50$, so $900^{900} = (900^{18})^{50} \equiv 1^{50} = 1 \pmod 19$.

(b) Find s and t so that $s \cdot 953 + t \cdot 859 = 1$.

$$\begin{array}{c|rrrrrrr} & 953 & 859 & 94 & 13 & 3 & 1 & 0 \\ s & 1 & 0 & 1 & -9 & 64 & -265 & \\ t & 0 & 1 & -1 & 10 & -71 & 294 & \\ & & & 94 & 13 & 3 & 1 & \end{array}$$

So $(-265)(953) + (294)(859) = 1$.

(c) Find $x < 3 \cdot 5 \cdot 7 = 105$ so that

$$x \equiv 2 \pmod 3, \quad x \equiv 4 \pmod 5, \text{ and } \quad x \equiv 4 \pmod 7.$$

We can find (by simple trial and error)

$$\begin{aligned} 35^{-1} &\equiv 2^{-1} \equiv 2 \pmod 3 \\ 21^{-1} &\equiv 1^{-1} \equiv 1 \pmod 5 \\ 15^{-1} &\equiv 1^{-1} \equiv 1 \pmod 7. \end{aligned}$$

So we set $x = 2 \cdot (2 \cdot 35) + 4 \cdot (1 \cdot 21) + 4 \cdot (1 \cdot 15) \bmod 105 = 284 \bmod 105 = 74$

(d) Find a closed form solution for $a_n = -a_{n-1} + 6a_{n-2}$ with $a_0 = 3$ and $a_1 = 1$.

The corresponding characteristic polynomial is

$$p(x) = x^2 + x - 6 = (x-2)(x+3)$$

so the general solution is $c_1(2^n) + c_2((-3)^n)$. The specific solution satisfies:

$$\begin{aligned} 3 &= c_1 + c_2 \\ 1 &= 2c_1 - 3c_2 \end{aligned}$$

Clearly, $c_1 = 2$ and $c_2 = 1$ is a solution and $f(n) = 2(2^n) + 1(-3)^n = 2^{n+1} + (-3)^n$.

(e) How many non-negative integer solutions are there to $x_1 + x_2 + x_3 = 19$ if $x_1 > 2$ and $x_2 < 7$.

The number of solutions to $x_1 + x_2 + x_3 = 19$ with $x_1 > 2$ is the same as the number of solutions to $x_1 + x_2 + x_3 = 16$ which is $\binom{16+3-1}{3-1}$. The number of solutions to $x_1 + x_2 + x_3 = 19$ with $x_1 > 2$ and $x_2 \geq 7$ is the same as the number of solutions to $x_1 + x_2 + x_3 = 9$ which is $\binom{9+3-1}{3-1}$. So the number of solutions to $x_1 + x_2 + x_3 = 19$ if $x_1 > 2$ and $x_2 < 7$ is

$$\binom{18}{2} - \binom{11}{2} = \frac{18 \cdot 17}{2} - \frac{11 \cdot 10}{2} = 98.$$

Problem 4 (Theory/Proofs; 40 points; 20 points each). Select **two** of the following four to complete. As above, you must make clear which three you choose.

(a) Show that $5n + 4$ and $4n + 3$ are relatively prime.

$$\gcd(5n+4, 4n+3) = \gcd(4n+3, n+1) = \gcd(n+1, n) = \gcd(n, 1) = 1$$

(b) Give a combinatorial argument for

$$0 = \sum_{i=0}^{n} (-1)^i \binom{n}{i}$$

Hint: Take a set A with $|A| = n$ and $a \in A$. For $B \subseteq A$ consider

$$f(B) = \begin{cases} B \cup \{a\} & \text{if } a \notin B \\ B - \{a\} & \text{if } a \in B \end{cases}$$

Show that f gives a 1-1 and onto correspondence between the even and odd sized subsets of A. Let E be the set of even sized subsets of A and O be the set of odd sized subsets of A. It is clear that $f_E = f|_E : E \to B$ and also that $f_O = f|_O : O \to E$ and that $f_E \circ f_O = \mathrm{id}_O$ and $f_O \circ f_E = \mathrm{id}_E$. Thus f_E is 1-1 and onto, thus $|E| = |O|$.

Now, using $\mathcal{P}_i(A)$ to mean the subsets of A of size i we have:

$$\begin{aligned} \sum_{i=0}^{n} (-1)^i \binom{n}{i} &= \sum_{i \le n \text{ even}} \binom{n}{i} - \sum_{i \le n \text{ odd}} \binom{n}{i} \\ &= \sum_{i \le n \text{ even}} |\mathcal{P}_i(A)| - \sum_{i \le n \text{ odd}} |\mathcal{P}_i(A)| \\ &= |E| - |O| = 0 \end{aligned}$$

(c) Give a combinatorial interpretation of the coefficient on x^n in

$$G(x) = (1 + x + x^3 + x^4 + \cdots)^4 = \left(\frac{1}{1-x}\right)^4 = \sum_{i=0}^{\infty} a_i x^i$$

Give the closed form expression for a_i based on your interpretation.

The coefficient on x^n is the number of ways to n as the sum of four non-negative integers, that is the number of solutions to $x_1 + x_2 + x_3 + x_4 = n$ and we know this to be

$$a_n = \binom{n+4-1}{n}$$

(d) Recall that in RSA you select two large primes p and q, set $n = pq$, $m = (p-1)(q-1)$, find $0 \leq e, d < m$ so that $ed \equiv 1 \pmod{m}$. You share (n, e) (for encryption) and have private (n, d) for decryption.

You would never share m since from it it is simple to compute d, nevertheless, show that given n and m it is "easy" to find p and q.

Note $m = pq - p - q + 1$ so $n - m = p + q - 1$. Let $s = p + q = (n - m) + 1$, this we have since we know n and m. We have $q = s - p$ so $n = pq = p(s - p) = p^2 - sp$. But now we can solve a quadratic to find p.