

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) _____ $13x + 9 \equiv -x + 2 \pmod{7}$ for all x .
- (b) _____ It is possible for a to have an inverse modulo b while b fails to have an inverse modulo a .
- (c) _____ If $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$ where p and q are distinct primes, then $x \equiv a \cdot b \pmod{p \cdot q}$.
- (d) _____ If $n + 1$ distinct integers are taken from the integers $1, 2, \dots, 2n$, then at least one pair of consecutive integers must be chosen.
- (e) _____ $G(X) = (1 + x)^n$ is a generating function for $a_m = \binom{n}{m}$.
- (f) _____ $a_n = 3 \cdot a_{n-1} + 2 \cdot a_{n-3}$ is a linear, homogeneous, 2nd-degree recurrence relation.
- (g) _____ 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.

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?

- ☐ $a + b \equiv (a \bmod n) + (b \bmod n) \pmod{n}$
- ☐ $a \cdot b \equiv (a \bmod n) \cdot (b \bmod n) \pmod{n}$
- ☐ $a^b \equiv (a \bmod n)^{(b \bmod n)} \pmod{n}$
- ☐ $b - a \equiv (b \bmod n) - (a \bmod n) \pmod{n}$.

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

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

(c) Which of the following have solutions?

- ☐ $x^2 \equiv 5 \pmod{7}$.
- ☐ $x^2 \equiv 7 \pmod{5}$.
- ☐ $x^2 \equiv 7 \pmod{11}$.
- ☐ $x^2 \equiv 11 \pmod{7}$.

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

- ☐ 500^2
- ☐ 1001^2 .
- ☐ 499^2 .
- ☐ 499 .

(e) Which of the following equations hold?

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

- (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.

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

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

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

- (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 $900^{900} \bmod 19$.

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

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

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

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

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

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.

(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 .

- (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.

- (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 .