Discrete Mathematics

COMS 3203 – Fall 2017

http://www.cs.columbia.edu/~amoretti/3203

Practice Exam # 2

Solve any five problems for full marks. **Good luck and don't panic!** If something is taking too long, move on to the next question. Note that this is a sample exam and while it bears some similarity with the real exam, the two are not isomorphic.

Problem 1

Evaluate the three expressions below.

1. *Hint:* use the Binomial Theorem:

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} \tag{1}$$

2. *Hint:* use the Geometric series:

$$\sum_{k=0}^{\infty} p(1-p)^k \tag{2}$$

3. *Hint:* use the Binomial Theorem:

$$\sum_{k=0}^{\infty} \binom{k+s-1}{k} (1-a)^s a^k \tag{3}$$

Problem 2

1. Prove that if $a' \equiv a \bmod n$ and $b' \equiv b \bmod n$ then $(a' \bmod n) \cdot (b' \bmod n) \equiv (a \cdot b) \bmod n$.

2. Does this operation define a group? Prove or disprove.

Problem 3

1. Consider the set $\mathbb{R}^*$ defined as $\mathbb{R} - \{0\}$. Is $(\mathbb{R}^*, +)$ a group? What about $(\mathbb{R}, \times)$? Prove or provide a counter example.

2. Let $\mathcal{S} = \mathbb{R} - \{-1\}$ and define the operation $a * b = a + b + a \times b$. Is $(\mathcal{S}, *)$ a group? Prove or provide a counter example.

Problem 4

Consider $\mathbb{Z}_p$ and the function $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ defined $f_a(x) = ax$. Write the functional digraph when $a = 3$ and $p = 11$. What do you notice about the cycle lengths? What happens when $a = 4$ and $p = 17$?

Problem 5

1. Fermat's Little Theorem states that a$^{p-1} - 1$ is an integer multiple of p:

$$a^{p-1} \equiv 1 (\mod p) \tag{4}$$

   Use this to show that $a^p \equiv a(\mod p)$. Give an example of an integer which satisfies Fermat's Little Theorem but is not prime.

2. Find an example of integers m, n, a, b where $gcd(m, n) \neq 1$ so that $x \equiv a(\mod m)$ and $x \equiv b(\mod n)$ has no solutions, and an example of m, n, a, b as above where the system has more than one solution.

Problem 6

Euler's Totient function $\phi(m)$ counts the numbers up to m relatively prime to m. Prove for any prime p:

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a\Big(1 - \frac{1}{p}\Big) \tag{5}$$

Problem 7

By the fundamental theorem of arithmetic, n can be factorized into m prime numbers.

$$n = \prod_{i=1}^{m} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \tag{6}$$

Use this to show that for $n \in \mathbb{Z}$ where $n > 1$:

$$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_m}\Big) \tag{7}$$