CSM 70 — Discrete Mathematics and Probability Theory

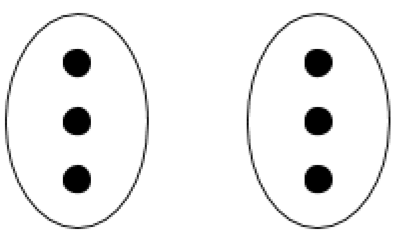
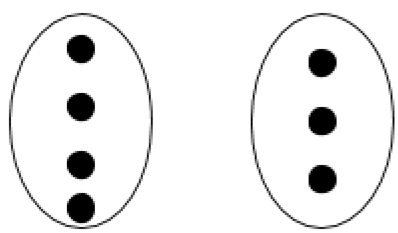
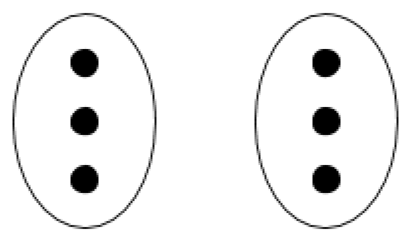
Spring 2016 — Bijections, FLT, CRT, Polynomials — **Worksheet 5**

Key Terms

- one to one
- onto
- bijection
- Fermat's Little Theorem
- Secret Sharing

I. Bijections

Draw mappings between the two sets that satisfy the conditions below.

		
One to one AND NOT onto	Onto AND NOT one to one	One to one AND onto (bijection)

Describe a function that is injective but not surjective. How about a function that is surjective but not injective?

Note: Z_n denotes the integers mod *n*: {0, …, *n*-1}
Note: in the following questions, the appropriate modulus is taken after applying the function

Are the following functions bijections from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{12}$?

f(x) = 7x

f(x) = 3x

f(x) = x - 6

Are the following functions are injections from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{24}$?

f(x) = 2x

f(x) = 6x

f(x) = 2x + 4

Which of the following functions are surjections from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{6}$?

f(x) = $\lfloor x/2 \rfloor$

f(x) = x

f(x) = $\lfloor x/4 \rfloor$

Why can we not have a surjection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{24}$ or an injection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{6}$?

II. FLT

Fermat's Little Theorem: For any prime p and any a $\in$ {1, 2, …, p-1}, we have $a^{p-1} \equiv 1 \bmod p$.

Exercises:

1) Find 3^{5000} (mod 11)

2) Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ (mod 7)

3) Show that $n^7 - n$ is divisible by 42 for any integer n

III. <u>CRT</u>

Find an integer x such that x is congruent to 3 mod 4 and 5 mod 9.

Prove the Chinese Remainder Theorem.

Theorem: Let p and q be coprime. Then the following system of equations has a unique solution for x modulo pq

$$x = a \pmod{p} \qquad (1)$$

$$x = b \pmod{q} \qquad (2)$$

The supermarket has a lot of eggs, but the manager is not sure exactly how many he has. When he splits the eggs into groups of 5, there are exactly 3 left. When he splits the eggs into groups of 11, there are 6 left. What is the minimum number of eggs at the supermarket?

IV. Polynomials

Fundamental properties of polynomials:

Property 1: A non-zero polynomial of degree d has at most __________ roots

Property 2: Given d + 1 pairs $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$ where all x's are distinct there is a unique polynomial p(x) of degree at most __________ such that $p(x_i) = y_i$ for i between 1 and d + 1

How many points does it take to uniquely determine a line? __________

Lagrange Interpolation:

We want to build a polynomial that passes through some given points.

Say we are given points $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$ and want to find a degree d polynomial that goes through those points.

$$\Delta 1 = y_1 * \frac{(x - x_2) \dots (x - x_{d+1})}{(x_1 - x_2) \dots (x_1 - x_{d+1})} \quad , \dots , \quad \Delta d{+}1 = y_1 * \frac{(x - x_1) \dots (x - x_d)}{(x_{d+1} - x_1) \dots (x_{d+1} - x_d)}$$

So the polynomial we are looking for must be the sum of the above delta's.

Let's do a simple example: What degree 1 polynomial goes through (1, 2) and (4, 10)? Just write out the deltas:

$\Delta 1 =$

$\Delta 2 =$

Prove that the polynomial produced by Lagrange interpolation of d+1 points is the unique degree d polynomial through those points.

Counting Polynomials

What is a Galois Field?

If you are working in GF(m) where m is a prime, how many polynomials of at most degree 3 are there?

Now suppose you are given three out of the four points. How many degree 3 polynomials go through these three points?

Secret Sharing

Scheme Conditions:

(1) Any group of k officials can pool their information to figure out the secret
(2) No group of k-1 or fewer officials have any information about the secret

If you have a group of n officials, choose a polynomial P(x) of degree _________ such that P(0) = s and give out P(1), …, P(n) to the officials.

Exercises

1) How many different polynomials of degree d over GF(p) are there if we know k values, where k <= d?

2) Your points are (2, 5), (1, 6), (4, 0). First, set up a linear equation that you could solve in order to find the unique ______ degree polynomial which goes through these points. After, solve and find the polynomial that passes through the points. GF(7)

3) Secret sharing is a crucial application of Polynomials. We have 20 TAs and 35 readers, and we want to share a secret among them such that either 2 or more TAs, at least 1 TA and at least 3 readers, or at least 6 readers can reconstruct the secret. Describe such a scheme.