CSM 70 Discrete Mathematics and Probability Theory

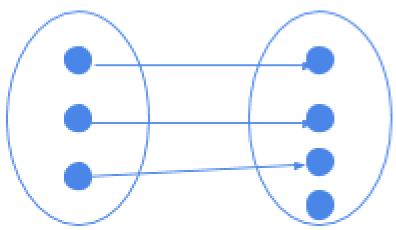
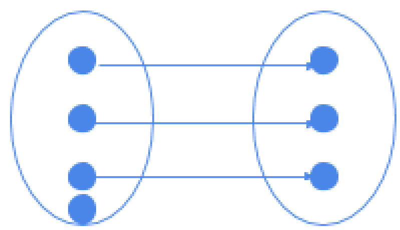
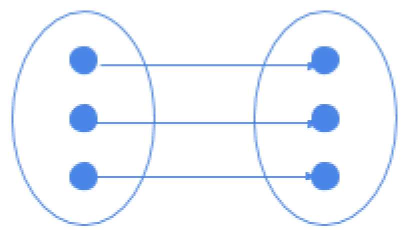
Spring 2016 Bijections, FLT, Polynomials **Worksheet 5**

Key Terms

one to one
onto
bijection

Fermat's Little Theorem
Secret Sharing

I. **Bijections**

		
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?

e^x: $\mathbb{R} \longrightarrow \mathbb{R}$ is injective (one to one) but not surjective (onto) because while all real numbers map to something, nothing will map to 0 and negative numbers.

x^2: $\mathbb{R} \longrightarrow \mathbb{R}^+$ is surjective (onto) but not injective (one to one) because while all positive real numbers have something mapping to them, 4 has -2 and 2 mapping to it.

Note 1: Z_n denotes the integers mod n: $\{0, \ldots, n\text{-}1\}$

Note 2: in the following questions, the appropriate modulus is taken after applying the function

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

$f(x) = 7x$ Yes: the mapping works

$f(x) = 3x$ No: $f(0) = f(4) = 0$

$f(x) = x - 6$ Yes: can see it's just $f(x) = x$, shifted by 6

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

$f(x) = 2x$ Yes: any two x1 and x2 will not equal each other as long as x1 != x2

$f(x) = 6x$ No: 0 and 4 both map to 0

$f(x) = 2x + 4$ Yes: same as 2x, except shifted

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

$f(x) = \lfloor x/2 \rfloor$ Yes: plug in every even number 0

$f(x) = x$ Yes: plug in 0 through 5

$f(x) = \lfloor x/4 \rfloor$ No: the largest value we can get is f(12) which equals 3

Why can we not have a surjection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{24}$ or an injection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{6}$?
Because there are more values in $\mathbb{Z}_{24}$ than $\mathbb{Z}_{12}$, it is impossible for the values in $\mathbb{Z}_{12}$ to map to every value in Z_{24}. Similarly, because there are more values in $\mathbb{Z}_{12}$ than $\mathbb{Z}_{16}$, we cannot have all values map to unique values.

II. FLT

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

Proof from notes:

Claim: The function ax mod p is a bijection where $x \in \{1, 2, \dots, p-1\}$

The domain and range of the function are the same set, so it is enough to show that if $x \not\equiv x'$ then $ax \pmod p \not\equiv ax' \pmod p$.

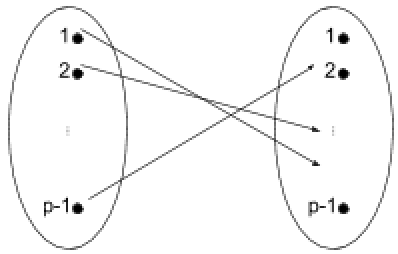
Assume that $ax \pmod p \equiv ax' \pmod p$.

Since $\gcd(a, p) = 1$, a must have an inverse: $a^{-1} \pmod p$

$$ax \pmod p \equiv ax' \pmod p$$
$$a^{-1}ax \pmod p \equiv a^{-1}ax' \pmod p$$
$$x \pmod p \equiv x' \pmod p$$

This contradicts our assumption that $x \not\equiv x' \pmod p$. Therefore f is a bijection.

We want to use the above claim to show that $a^{p-1} \equiv 1$ mod p. Note that now we have the following picture:



So if we multiply all elements in the domain together this should equal the product of all the elements in the image:

$$1 * 2 * \ldots * (p-1) \equiv (1a) * (2a) * \ldots * ((p-1)a) \pmod p$$
$$(p-1)! \equiv a^{p-1} * (p-1)! \pmod p$$
$$1 \equiv a^{p-1} \pmod p \ ▮$$

Exercises:

1) Find $3^{5000} \pmod{11}$

   $(3^{10})^{500} \pmod{11} = 1^{500} \pmod{11} = 1$

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

   By FLT:

   $2^6 \equiv 1 \pmod 7$
   $3^6 \equiv 1 \pmod 7$
   $4^6 \equiv 1 \pmod 7$
   $5^6 \equiv 1 \pmod 7$
   $6^6 \equiv 1 \pmod 7$

   Apply the above facts to simplify each portion of the equation:

   $2^{20} = 2^2 * (2^6)^3 \rightarrow 2^{20} \pmod 7 \equiv 2^2 \pmod 7 \equiv 4 \pmod 7$
   $3^{30} = (3^6)^5 \rightarrow 3^{30} \pmod 7 \equiv 1 \pmod 7$
   $4^{40} = 4^4 * (4^6)^6 \rightarrow 4^{40} \pmod 7 \equiv 4^4 \pmod 7 \equiv 4 \pmod 7$
   $5^{50} = 5^2 * (5^6)^8 \rightarrow 5^{50} \pmod 7 \equiv 5^2 \pmod 7 \equiv 4 \pmod 7$
   $6^{60} = (6^6)^{10} \rightarrow 6^{60} \pmod 7 \equiv 1 \pmod 7$

   $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod 7 \equiv 4 + 1 + 4 + 4 + 1 \pmod 7$
   $\equiv 14 \pmod 7 \equiv 0 \pmod 7$

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

   $42 = 7 * 3 * 2 \leftarrow$ these factors are prime so let's apply FLT!!

   $n^7 \equiv n \pmod 7$
   $n^3 \equiv n \pmod 3$
   $n^2 \equiv n \pmod 2$

   We're interested in n^7 so let's modify the bottom two equations to write n^7 in mod 3 and mod 2

   $n^7 \equiv n^3 * n^3 * n \equiv n * n * n \equiv n^3 \equiv n \pmod 3$
   $n^7 \equiv n \pmod 3$

   $n^7 \equiv n^2 * n^2 * n^2 * n \equiv n * n * n * n \equiv n^2 * n^2 \equiv n * n \equiv n^2 \equiv n \pmod 2$
   $n^7 \equiv n \pmod 2$

$n^7 \equiv n \pmod 7$
$n^7 \equiv n \pmod 3$
$n^7 \equiv n \pmod 2$

Wouldn't it be great if the above equations implied that $n^7 \equiv n \pmod{7 * 3 * 2}$?
Let's try to prove that
Claim: If

$x \equiv y \pmod{a_1}$
$x \equiv y \pmod{a_2}$
…
$x \equiv y \pmod{a_n}$

are true and $a_1, \ldots, a_n$ are coprime then $x \equiv y \pmod{a_1 a_2 \ldots a_n}$
$x \equiv y \pmod{a_i} \Rightarrow x = y + c_i a_i$ for some constant c_i

$x = y + c_1 a_1$
$x = y + c_2 a_2$
…
$x = y + c_n a_n$

But this implies that $x = c * \mathrm{lcm}(a_1, \ldots, a_n) + y$
Since $a_1, \ldots, a_n$ are coprime, $\mathrm{lcm}(a_1, \ldots, a_n) = a_1 a_2 \ldots a_n$
So we get $x = c * a_1 a_2 \ldots a_n + y$
Therefore $x \equiv y \pmod{a_1 a_2 \ldots a_n}$

We can now say that $n^7 \equiv n \pmod{7*3*2} \equiv n \pmod{42}$.

III. <u>CRT</u>

Find an integer x such that x is congruent to 3 mod 4 and 5 mod 9.
One way is to find a number that is 1 mod 4 and 0 mod 9. To do that, we need to have $9x = 1 \pmod 4$, which works when $x = 1$, so the number is 9. We do the same with 0 mod 4 and 1 mod 9, so $4x = 1 \pmod 9$. This yields $x = 7$, or 28. Our answer is then $3 * 9 + 5 * 28 \pmod{36}$.

Prove the Chinese Remainder Theorem.

Find x such that:

$x = 2 \pmod 5$
$x = 3 \pmod 7$

Chinese Remainder Theorem tells us that there is always a unique solution up to a certain modulus.

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

$x = a \pmod p$ (1)
$x = b \pmod q$ (2)

Proof:
Let $p_1 = p^{-1} \pmod q$ and $q_1 = q^{-1} \pmod p$
We know that such p_1 and q_1 exist since p and q are coprime.
Let $y = aqq_1 + bpp_1 \pmod{pq}$.
If such a y exists then it satisfies equations (1) and (2).

$y \pmod p = aqq_1 + bpp_1 \pmod p = aqq_1 \pmod p = a \pmod p$

$y \pmod q = aqq_1 + bpp_1 \pmod q = bpp_1 \pmod q = b \pmod q$

Therefore y is a valid solution for x.
Now we must show that no other solutions exist for equations (1) and (2)
If $z = a \pmod p$ then $z - y$ is a multiple of p.
If $z = b \pmod q$ then $z - y$ is also a multiple of q.
p and q are coprime so $z - y$ is a multiple of pq and $z = y \pmod{pq}$.

Exercises

1) <u>How many eggs?</u>
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?

y_1 = 1 (mod 5), y_2 = 0 (mod 5)
y_1 = 0 (mod 11), y_2 = 1 (mod 11)
y_1 = 11p' (mod 55), y_2 = 5q' (mod 55)
p' = 11^(-1) (mod 5), y_2 = 5^(-1) (mod 11)
p' = 1 (mod 5), y_2 = 9 (mod 11)

x = 3 * 1 + 9 * 11 = 102 (mod 55)

IV. Polynomials

Fundamental properties of polynomials:

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

Property 2: Given d + 1 pairs $(x_1, y_1) \ldots (x_{d+1}, y_{d+1})$ where all x's are distinct there is a unique polynomial p(x) of degree at most d 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? 2

Lagrange Interpolation:

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

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

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:

$\Delta 1 = 2 * (x - 4) / (1 - 4)$

$\Delta 2 = 10 * (x - 1)/(4 - 1)$

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

Assume that p is the polynomial produced by Lagrange interpolation and q is another polynomial that goes through the same points. We have that p(xi) = q(xi) = yi for $1 \le i \le d+1$. Then r(x) = p(x) - q(x) is a polynomial of at most degree d with d+1 roots. This contradicts Property 1, so our assumption must have been incorrect and q(x) cannot exist.

How Many Polynomials?

What is a Galois Field? numbers modulo a prime

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

There are two ways to uniquely define a polynomial:

$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ OR $p(x) = (x - a_0)(x - a_1)(x - a_2)(x - a_3) = 0$

a_0, a_1, a_2, a_3 can take on any of the m values in GF(m). So there are m^4 polynomials.

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

How many options are there for the fourth point? m

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 k - 1 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?

   p^(d+1-k). We need d+1 points to make the polynomial, and if we know 0 points, then every point can be anything in the span of p. As soon as we start finding more points, the amount of non-fixed points becomes less and less, until k = d+1, where we are left with one polynomial.

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)

   Δ2 = (x − 1)(x − 4) / (2 − 1)(2 − 4) = x^2 − 5x + 4 / (1)(-2) = 3(x^2 - 5x + 4) = 3x^2 + 6x + 5

   Δ1 = (x − 4)(x − 2) / (1 − 4)(1 − 2) = x^2 − 6x + 8 / (-3)(−1) = 5(x^2 - 6x + 8) = 5x^2 + 5x + 5

   Δ4 = (x − 2)(x − 1) / (4 − 2)(4 − 1) = x^2 − 3x + 2 / (2)(3) = 6(x^2 - 3x + 2) = 6x^2 + 6x + 4

   5Δ2 + 6Δ1 + 0Δ4 = 4(3x 2 + 4x + 1) + (3x 2 + 3x) + 2(4x 2 + 3x)

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.

A TA is essentially 3 readers, so if we make a polynomial of degree 5 such that P(0) is the secret, each reader gets one point while each TA gets 3 points.