BIJECTIONS, FLT, RSA, POLYNOMIALS, SECRET SHARING

COMPUTER SCIENCE MENTORS 70

September 26 to September 30, 2016

1 Bijections

1.1 Introduction

1. Draw an example of each of the following situations

One to one AND NOT onto (injective but not surjective)	Onto AND NOT one to one (surjective but not injective)	One to one AND onto (bijection, i.e. injective AND surjective)

2. Describe a function that is injective but not surjective and the set over which this applies. How about a function that is surjective but not injective?

Note 1: Z_n denotes the integers mod n: $\{0, \ldots, n-1\}$
Note 2: in the following questions, the appropriate modulus is taken after applying the function

1.2 Questions

1. Are the following functions **bijections** from Z_{12} to Z_{12}?
   a. $f(x) = 7x$

   b. $f(x) = 3x$

   c. $f(x) = x - 6$

2. Are the following functions **injections** from Z_{12} to Z_{24}?
   a. $f(x) = 2x$

   b. $f(x) = 6x$

   c. $f(x) = 2x + 4$

3. Are the following functions **surjections** from Z_{12} to Z_6? (Note: that $\lfloor x \rfloor$ is the floor operation on x)
   a. $f(x) = \lfloor \frac{x}{2} \rfloor$

   b. $f(x) = x$

   c. $f(x) = \lfloor \frac{x}{4} \rfloor$

4. Why can we not have a surjection from Z_{12} to Z_{24} or an injection from Z_{12} to Z_6?

2 Fermat's Little Theorem

2.1 Introduction

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

1. Prove Fermat's Little Theorem.

2.2 Questions

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

3 RSA

3.1 Questions

1. **How does RSA work?**

   a. Alice wants to send Bob a message $m = 5$ using his public key ($n = 26$, $e = 11$). What cipher text E(m) will Alice send?

   b. What is the value of d (Bobs private key) in this scheme? Note that traditional RSA schemes use much larger prime numbers, so its harder to break n down into its prime factors than it is in this problem.

2. In RSA, if Alice wants to send a confidential message to Bob, she uses Bobs public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is (3, 77). And then Bob chose $d = 26$ so his private key is (26, 77).
   Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

3. **Coin tosses over text messages**
   You and one of your friends want to get your hands on the new gadget thats coming out. One of you has to wait in line overnight so that you have a chance to get the gadgets while they last. In order to decide who this person should be, you both agree to toss a coin. But you wont meet each other until the day of the actual sale and you have to settle this coin toss over text messages (using your old gadgets). Obviously neither of you trusts the other person to simply do the coin toss and report the results.

   How can you use RSA to help fix the problem?

4 Polynomials

4.1 Introduction

1. If polynomial P(x) has degree n - 1 then we can uniquely reconstruct it from any n distinct points.
2. If a polynomial P(x) has degree n - 1 then it can be uniquely described by its n coefficients

4.2 Questions

1. Define the sequence of polynomials by $P_0(x) = x+12$, $P_1(x) = x^2-5x+5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$. (For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)
   (a) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in N$.

   (b) Show that, for every prime q, if $P_{2013}(x) \not\equiv 0 \pmod{q}$, then $P_{2013}(x)$ has at most 2013 roots modulo q.

5 Secret Sharing

5.1 Questions

1. Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted and we know that:
   (a) Both TAs should be able to access the answers
   (b) All 3 Readers can also access the answers
   (c) One TA and one Reader should also be able to do the same

   Design a secret sharing scheme to make this work.

2. An officer stored an important letter in her safe. In case she is killed in battle, she decides to share the password with her troops. Everyone knows there are 3 spies among the troops, but no one knows who they are except for the three spies themselves.The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

   1. When M of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
   2. The 3 spies must not be able to open the safe all by themselves.

   Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest M? Show your work and argue why your scheme works and any smaller M couldnt work.