

# CRT, BIJECTIONS, FLT, RSA

---

## META

September 18 to September 22, 2017

---

### 1 General Comments

---

#### 1. Logistics

- There will be no sections on Monday; the midterm is then.

#### 2. Bijections

- Make sure that they understand one-to-one = injective and onto = surjective
- Make sure to go over what it means to be a well-defined function, this is *essential* to understanding injective/surjective.
- Don't be afraid to spend a good chunk of time talking through the drawings.
- Many students will assume that surjections are just injections from the codomain to the domain (they are not!).
- The why is this mapping (not) bijective questions are important
- Make sure they're comfortable with bijections (this will be especially important in RSA)
- Emphasize that bijection is equivalent to invertibility.

#### 3. FLT

- Last question is kind of repetitive skip if low on time

#### 4. RSA

- Sections earlier in the week may not have strong RSA practice, so don't spend too much time if they aren't very familiar with it
- If you don't get to the RSA questions, briefly explain how it works on a high-level

- Make sure they understand how RSA actually works the implementation questions test for that pretty well
- Draw a picture! Ask what is public? What is private?
- Coin tosses question is interesting. Tests if they actually understand why RSA works, rather than just how its implemented
- Go over the proof from notes on how/why RSA works

#### 5. CRT

- This may or not be covered.
- This is something that students have a bit of trouble with, but I'd say work through a simple case.

#### 6. Polynomials

- Monday-Wednesday will probably not get to this

#### 7. Secret Sharing

- This is in there just for Friday people

#### 8. Mandatory questions you have to get to

- Bijections: Why you cant find injections/bijections between some spaces
- FLT: FLT Proof
- RSA: That one proof about how it works and applies FLT
- Polynomials: Only do this if you have time, if you get to this do a vanilla intro
- Secret Sharing: Again do a vanilla intro if you get to this section