

# 15-251: Great Theoretical Ideas In Computer Science

---

## Recitation 7

### Test Next Monday

Test 2 is next week in recitation. The format will be the same as in Test 1. It covers all lectures until (and including) Lecture #17 (on Tuesday), though the focus will be on material not covered in Test #1.

### RSA Encryption

In lecture, we saw how RSA encryption is used. There are many important quantities used in this algorithm:

- $p, q$ : Two very large prime numbers.
- $n$ :  $n = pq$  is part of the public key.
- $\phi(n)$ : Since  $p, q$  prime,  $\phi(n) = (p - 1)(q - 1)$ .
- $e$ :  $e$ , the “encryption exponent” also part of the public key, is some member of  $\mathbb{Z}_{\phi(n)}^*$
- $d$ :  $d$ , the private key or “decryption exponent”, is the inverse of  $e$  in  $\mathbb{Z}_{\phi(n)}^*$ , i.e.,  $e \times d \equiv_{\phi(n)} 1$
- $m$ : This is the message that will be sent

To send a message to Alice using Alice’s public key  $(n, e)$ , Bob sends  $m^e \bmod n$ .  
Alice decrypts his message by calculating  $(m^e)^d \bmod n$ .

1. If Alice chose  $p = 7, q = 11, e = 13$ , how would she decode the encrypted message 3?
2. Now encrypt the message 68. (Treat this as a decimal value).

### Symmetry Group of a Circle

Recall from lecture that  $D_n$  is the group of all rotations and reflections of a regular  $n$ -gon, where the operation is composition. Let  $D_\infty$  be the group of all rotations and reflections of a circle.

3. How many elements are in  $D_\infty$ ?
4. What is the identity of  $D_\infty$ ?
5. How many elements have order 1? What are they?
6. How many elements have order 2? What are they?
7. How many elements have order 3? What are they?
8. How many elements have finite order? What are they?
9. How many elements have infinite order? What are they?
10. Can  $D_\infty$  be generated by a single element?

## Subgroups

We use the notation  $H \leq G$  to say " $H$  is a subgroup of  $G$ ".

11. Let  $H \subseteq G$ . Prove that  $H \leq G$  if and only if  $H$  is nonempty and for all  $x, y \in H$ ,  $xy^{-1} \in H$ .  
*Note that this property is useful when proving that a subset of a group is a subgroup.*
12. Prove that if  $H \leq G$  and  $K \leq G$ , then  $H \cap K \leq G$ .