Week 8 Friday

Make sure you’re sitting next to someone!

Favorite Candy

Make sure you know your neighbors' names(s), and then discuss:

Do you have a favorite type of candy, or did you when you were younger? What is it? What are some memories you associate with it? Is it a type of candy that's still around? Do you still like it?

RSA, continued

1. When generating his RSA public key, Bob secretly chooses primes p and q, but then he makes an unwise decision to reveal to you that the primes p and q that he chose satisfy the equation

$$(x-p)(x-q) = x^2 - 34x + 253.$$

Use this information to find $\phi(n)$ without factoring $n = pq$.

Order, Primitive Roots

2. Suppose a is an integer that is not divisible by 13. Which of the following cannot be the order a mod 13?

(A) 2

(B) 3

(C) 4

(D) 5

3. What is the order of 4 mod 13?

4. Which of the following is a primitive root of 17?

(A) 2

(B) 3

(C) 4

(D) None of the above