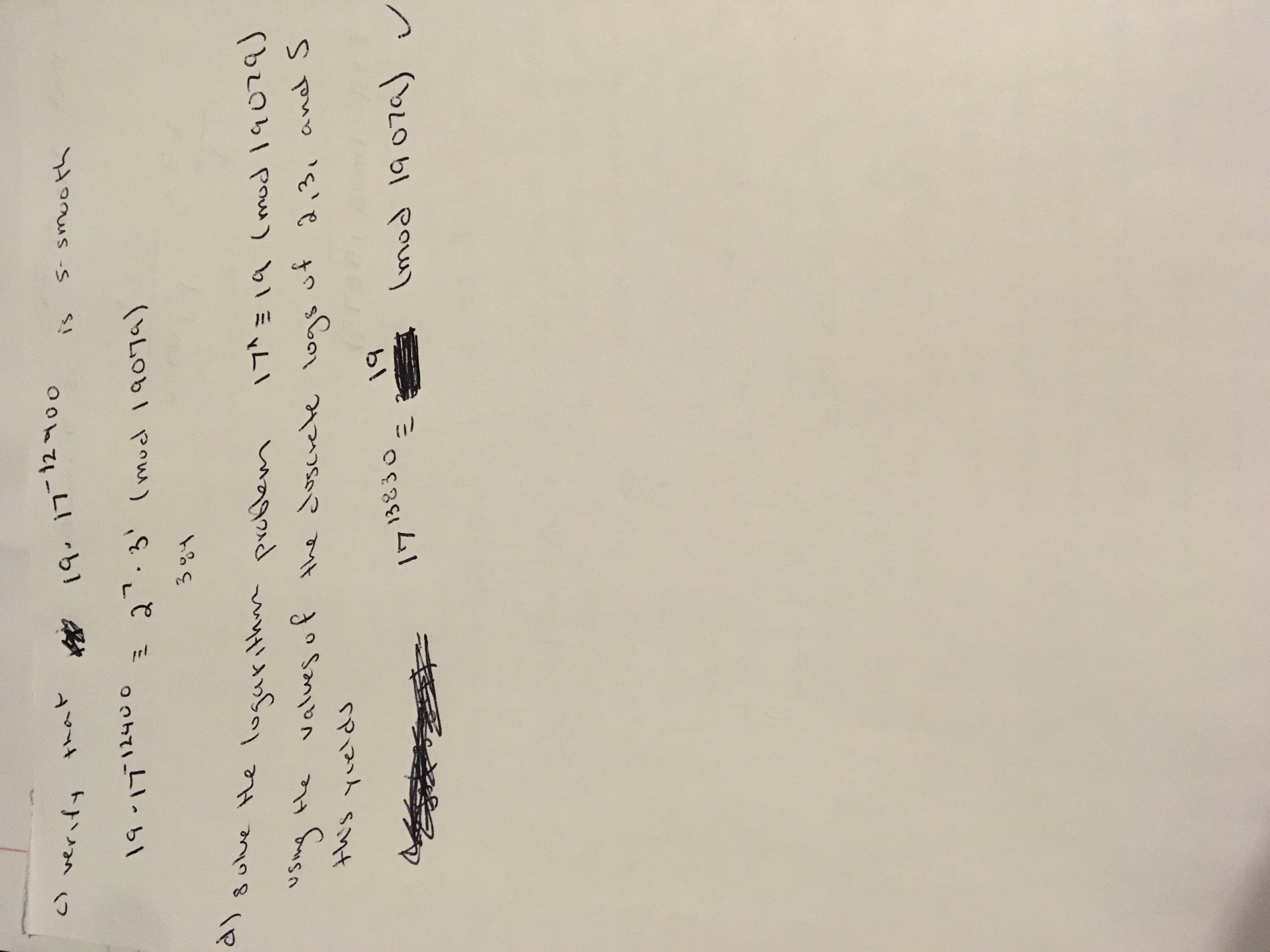
Homework 7 – Group 2

3.38

a.)

this means that it would be ≡ a mod p which satisfies the proof.

b.) i.) a = 116 , p = 587

ii.) a = 3217, p = 8672

III.) a = 9109, p = 10663

So we check 3502^2 mod 587 actually equals 1554 mod 10663.This means that this is not a quadratic residue modulo of 10663. However you can see that 3502^2 mod 10663 is actually equal to

-9109 mod 10663.

3.41

a) N = 1842338473, a = 1532411781

Since the ciphertext is not a quadratic residue to p then **plaintext = 1**

The ciphertext is a quadratic residue to p so **plaintext = 0**

The cipher text is not a quadratic residue to p so **plaintext = 1**

b) N = 3149, a = 2013

N = pq = 47\*67

The cipher text is not a quadratic residue to p so **plaintext = 1**

The ciphertext is a quadratic residue to p so **plaintext = 0**

The ciphertext is a quadratic residue to p so **plaintext = 0**

c) N = 781044643, a = 568980706

r =705130839, m = 1

**C = 517254876**

r = 631364468, m = 1

**C = 4308279**

r = 67651321, m = 0

**C =660699010**