Name: Solutions

Math 4400 Quiz 6

July 31, 2016

Instructions: You have until the end of class to complete this quiz. This quiz is two pages, and worth 20 points. Make sure to write your name at the top of the quiz. Show all of your work for full credit!

1. (a) (5 points) Is $(m = 13 \cdot 23, e = 5)$ a valid public key for RSA encryption? Why or why not?

$\varphi(m) = 12 \cdot 22 = 264$

$\gcd(5, 264) = 1$, ~~so~~ yes.

(b) (5 points) If yes, find the corresponding private key. If no, give an example of a valid public key.

Private key $= (13 \cdot 23, d)$ where $d \cdot e \equiv 1 \mod 264$

$264 = 52 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$\rightsquigarrow 53 \cdot 5 - 264 = 1$

$\rightsquigarrow d = 53$

$$\boxed{(13 \cdot 23, 53)}$$

"QR"

2. (10 points) Quadratic reciprocity states: if p and q are odd primes, then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & p \equiv 1 \mod 4, \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right), & q \equiv p \equiv 3 \mod 4 \end{cases}$$

Use this to prove

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & q \equiv 1 \mod 4 \\ \left(\frac{-q}{p}\right), & q \equiv 3 \mod 4 \end{cases}$$

If $q \equiv 1 \mod 4$, then, by QR, $\left(\frac{p}{q}\right) = (q/p)$, as desired.

If $q \equiv 3 \mod 4$, then

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{if } p \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right), & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$= \left(\frac{p}{q}\right)$$ by QR.