Problem Set 5, Question 4

Question 4 on Problem Set 5 asks for a proof of the second of three conditions that the RSA encryption scheme must meet to be considered secure and reliable.

**Condition 2.** The value of $x$ calculated in Step 9 of the RSA algorithm should always equal the value of $x$ that Bob selects in Step 6.

Showing that this condition is satisfied requires the use of the following two theorems.

**Theorem 2.** Let $p$ and $q$ be distinct prime numbers. For any integer $a$,

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq},$$

where $k$ is any positive integer.

**Theorem 4.** For any integers $a$ and $b$ and any positive integer $m$,

$$(a \pmod{m})^b \pmod{m} = a^b \pmod{m}.$$

Checking the calculation in Step 9 of the RSA algorithm, we see that we want to show that $y^d \pmod{m} = x$. Let’s start with the left side of that equation and try to simplify our way to $x$.

$$y^d \pmod{m} = (x^e \pmod{m})^d \pmod{m} \quad \text{[since } y = x^e \pmod{m}]$$

$$= (x^e)^d \pmod{m} \quad \text{[by Theorem 4]}$$

$$= x^{ed} \pmod{m}.$$

We’ll need to show that this simplifies to $x$, but to do that, we’ll need to see what Theorem 2 looks like in this context. Recall from the RSA algorithm that $n = (p - 1)(q - 1)$ and $m = pq$, and so Theorem 2 tells us that for any integers $a$ and $k$,

$$a^{kn+1} \equiv a \pmod{m}.$$

Does that $kn + 1$ look familiar? When proving Condition 1 earlier in the Problem Set, we noted that $ed \equiv 1 \pmod{n}$ and so $ed = kn + 1$ for some integer $k$. It follows that $x^{ed} = x^{kn+1}$. Thus

$$x^{ed} = x^{kn+1} \equiv x \pmod{m}$$

by Theorem 2.

Since $x^{ed}$ is congruent to $x \pmod{m}$ and since $0 \leq x < m$ (because it was selected that way in Step 6 of the RSA algorithm), it follows that $x^{ed} \pmod{m} = x$. Why? Recall that $a \pmod{b}$ is the remainder when you divide $a$ by $b$, which is equal to the number congruent to $a \pmod{b}$ that is between 0 and $b - 1$. In this case, $x$ satisfies those two properties, that it is congruent to $x^{ed}$ and that it is between 0 and $m - 1$.

Putting it all together, we have that

$$y^d \pmod{m} = (x^e \pmod{m})^d \pmod{m}$$

$$= (x^e)^d \pmod{m}$$

$$= x^{ed} \pmod{m}$$

$$= x.$$
Thus, \( y^d \text{ MOD } m = x \), which proves Condition 2.

I’ll add that Theorem 2 can be proven by Fermat’s Little Theorem. Not Fermat’s “last” theorem, his “little” theorem. I won’t state that theorem here, or use it to prove Theorem 2, but you can Google if it you’re interested.

I will, however, prove Theorem 4, which lets us switch from “MOD” to “mod” in the argument above. The proof is messy, but see if you can follow. Note that whatever \( a \text{ MOD } m \) is, it must be congruent to \( a \text{ (mod } m) \). Thus

\[
a \text{ MOD } m \equiv a \text{ (mod } m).
\]

If two numbers are congruent, they’ll still be congruent when you raise them to the same power, and so

\[
(a \text{ MOD } m)^b \equiv a^b \text{ (mod } m).
\]

Let’s fiddle with the right side of that equation: Whatever \( a^b \text{ MOD } m \) is, it has to be congruent to \( a^b \text{ (mod } m) \), so we can replace the \( a^b \) in the right side of that equation with \( a^b \text{ MOD } m \):

\[
(a \text{ MOD } m)^b \equiv (a^b \text{ MOD } m) \text{ (mod } m).
\]

Note that \( (a^b \text{ MOD } m) \) has to be between 0 and \( m - 1 \), since it’s the result of a “MOD \( m \)” operation. Since it’s also congruent to \( (a \text{ MOD } m)^b \), it must equal \( (a \text{ MOD } m)^b \text{ MOD } m \).

Messy, right? To clarify a bit, let \( \alpha = (a \text{ MOD } m)^b \) and \( \beta = (a^b \text{ MOD } m) \). Then we’ve shown that \( \alpha \equiv \beta \text{ (mod } m) \) and that \( \beta \) is between 0 and \( m - 1 \). Then \( \beta \) must equal \( \alpha \text{ MOD } m \). Thus,

\[
(a \text{ MOD } m)^b \text{ MOD } m = a^b \text{ MOD } m,
\]

which proves Theorem 4.