Staple here!
CMSC 27100 Autumn 2015

Acknowledgement:

Name: Jaime Arana-Rochel
Section: 1

Homework #2

Q1

Problem: Show that there are composite numbers m such that $x^2 \equiv 1 \,(mod\, m)$ has solutions other than $x \equiv 1 \,(mod\, m)$ and $x \equiv -1 \,(mod\, m)$

Let the modulus m be 16. We need to find a value other than 1 and -1 that satisfies,

$$x^2 \equiv 1 \,(mod\, 16)$$

By inspection we find that when x=7 the congruence relation holds. Other composite numbers can be found for m such as 12. In which case we see that a solution to

$$x^2 \equiv 1 \,(mod\, 12)$$

is possible when x=5. Thus there are composite numbers m such that $x^2 \equiv 1 \,(mod\, m)$ has solutions other than $x \equiv 1 \,(mod\, m)$ and $x \equiv -1 \,(mod\, m)$.

Q3

a) One can construct pairs of integers that are inverses of each other modulo 11, taken from the positive integers less than 11 except 1 and 10, by calculation. Consider the integer 2. It's modular inverse,x, needs to satisfy the following congruence,

$$x2 \equiv 1 \,(mod\, 11)$$

This congruence holds when x=6. Thus one pair is (2,6). Following the same method for the rest of the integers, the pairs are: (2,6), (3,4), (5,9), and (7,8).

b) Using the result from part a, we can rewrite $10! \equiv -1 \,(mod\, 11)$ as

$$1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 \equiv -1 \,(mod\, 11)$$

$$1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \equiv -1 \,(mod\, 11)$$

$$10 \equiv -1 \,(mod\, 11)$$

Since this $10 \equiv -1 \,(mod\, 11)$ is true, then we've shown that $10! \equiv -1 \,(mod\, 11)$.

Q4

Find all solutions, if any, to the system of congruences: $x \equiv 5\,(mod\,6)$, $x \equiv 3\,(mod\,10)$, $x \equiv 8\,(mod\,15)$.

Because the moduli are not pairwise relatively prime to each other, we cannot use the remainder theorem unless we split the system of linear congruences such that the moduli *are* pairwise relatively prime. The following

$$x \equiv 5\,(mod\,6)$$

can be split into the equivalent two congruences

$$x \equiv 5\,(mod\,2) \qquad x \equiv 5\,(mod\,3)$$

The other two congruences in the system can be split as well such that are enlarged system of congruences is

$$x \equiv 5\,(mod\,2) \qquad x \equiv 5\,(mod\,3)$$
$$x \equiv 3\,(mod\,2) \qquad x \equiv 3\,(mod\,5)$$
$$x \equiv 8\,(mod\,3) \qquad x \equiv 8\,(mod\,5)$$

Even though this larger system has six congruences, when we pair them up such that their moduli are the same we find that they are equivalent. For example the following pair is equivalent to each other,

$$x \equiv 8\,(mod\,3) \qquad x \equiv 5\,(mod\,3)$$

We can thus rewrite this system as

$$x \equiv 5\,(mod\,2)$$
$$x \equiv 5\,(mod\,3)$$
$$x \equiv 3\,(mod\,5)$$

Now can use the Chinese Remainder Theorem method described in the book:
$m = 2 \cdot 3 \cdot 5 = 30 \quad M_1 = 30/2 = 15 \quad M_2 = 30/3 = 10 \quad M_3 = 30/5 = 6$
By inspection we see that 1 is an inverse of $(15\ mod\ 2)$, 1 is an inverse of $(10\ mod\ 3)$, and 1 is an inverse of $(6\ mod\ 5)$. Thus the solutions to the system are those x such that

$$x \equiv\ a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3\ =\ 5 \cdot 15 \cdot 1 + 5 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1\ =\ 143 \equiv\ 23\ (mod\ 30)$$

Q5

The quadratic residues of 11 can be found using calculation. We use the equation $x^2 \equiv a \ (mod\ 11)$ and try to find solutions for different integers. For example

$$1^2 \equiv a \ (mod\ 11) \quad a = 1$$

$$2^2 \equiv a \ (mod\ 11) \quad a = 4$$
$$3^2 \equiv a \ (mod\ 11) \quad a = 9$$
$$4^2 \equiv a \ (mod\ 11) \quad a = 5$$
$$5^2 \equiv a \ (mod\ 11) \quad a = 3$$
$$6^2 \equiv a \ (mod\ 11) \quad a = 3$$
$$7^2 \equiv a \ (mod\ 11) \quad a = 5$$
$$8^2 \equiv a \ (mod\ 11) \quad a = 9$$
$$9^2 \equiv a \ (mod\ 11) \quad a = 4$$
$$10^2 \equiv a \ (mod\ 11) \quad a = 1$$

We find that the quadratic residues repeat, and that the set of quadratic residues of 11 is ultimately $\{1, 3, 4, 5, 9\}$.

Q6

We noticed in the last problem that the set of quadratic residues repeat in reverse order after a certain point for odd prime 11, for integers $\{1...p-1\}$. Let's try the same for $p = 5$.

$$1^2 \equiv a \ (mod\ 5) \quad a = 1$$

$$2^2 \equiv a \ (mod\ 5) \quad a = 4$$
$$3^2 \equiv a \ (mod\ 5) \quad a = 4$$
$$4^2 \equiv a \ (mod\ 5) \quad a = 1$$

We notice that the set of residues start repeating at the halfway point of $\{1...p-1\}$. Thus, the number of residues of an odd prime p are $(p-1)/2$.