Problem Set #3

Due monday 30 September in Class

Exercise 1: (∗) 2 points
Find all solutions of the congruence $12x \equiv 3 \pmod{45}$.

Solution:
Since $\gcd(12, 45) = 3$ and $3 \equiv 0 \pmod{3}$, the equation has exactly three solutions in $\mathbb{Z}/45$. To find a solution, we need to solve:

$$4x \equiv 1 \pmod{15} \quad (1)$$

The inverse of 4 in $\mathbb{Z}/15$ can be found by Euclidean algorithm:

$$15 = 3 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$

and Euclidean equations performed backward are:

$$1 = 1 \cdot 4 - 1 \cdot 3$$
$$= 4 \cdot 4 - 1 \cdot 15$$

Thus, $4^{-1} \equiv 4 \pmod{15}$, and a solution of the equation (1) is $x \equiv 4 \pmod{15}$. Hence,

$$12x \equiv 3 \pmod{45} \iff x \equiv 4, 19, \text{ or } 34 \pmod{45}$$

Exercise 2: (**) 4 points
Find a solution of the system of congruences

$$2x \equiv 1 \pmod{5}$$
$$3x \equiv 4 \pmod{7}$$

Solution:
By applying Euclidean algorithm, we can find that $2^{-1} \equiv 3 \pmod{5}$ and $3^{-1} \equiv 5 \pmod{7}$. Thus, we need to solve:

$$x \equiv 3 \pmod{5}$$
$$x \equiv 6 \pmod{7}$$

Let $x = 5y + 7z$. Then, the above system of equation becomes

$$2z \equiv 3 \pmod{5}$$
\[ 5y \equiv 6 \mod 7 \]

Solve these equations like what we did in the previous problem, then we have \( y \equiv 4 \mod 7 \) and \( z \equiv 4 \mod 5 \). Hence, \( x \equiv 5 \cdot 4 + 7 \cdot 4 \equiv 13 \mod 35 \).

**Exercise 3: (***) 5 points**

Prove that for each \( n \geq 1 \), there are exactly four non-negative integers of \( n \) digits such that the last \( n \) digits of its square is equal to itself. In this problem, we also consider 000 or 021 as integers of 3 digits. When \( n = 3 \), non-negative integers satisfying such property are 000, 001, 376, and 625. Find these integers for \( n = 5 \).

**Solution:**

First, note that in this problem, an integer \( m \) is a non-negative integer of \( n \) digits if and only if \( 0 \leq m < 10^n \) is true. Suppose that \( m \) is a non-negative integer of \( n \) digits such that the last \( n \) digits of \( m^2 \) is \( m \). This means that \( 10^n | m^2 - m = m(m - 1) \). Neither 2 nor 5 can divide two consecutive numbers, so there are only four cases;

- Case 1: \( 10^n | m \),
- Case 2: \( 10^n | m - 1 \),
- Case 3: \( 5^n | m \) and \( 2^n | m - 1 \),
- Case 4: \( 2^n | m \) and \( 5^n | m - 1 \).

**Case 1:** Since \( m < 10^n \), we can conclude that \( m = 0 \). **Case 2:** Again, since \( m < 10^n \), we can conclude that \( m = 1 \). **Case 3:** Write \( m = 5^n r \). Then, since \( m < 10^n \), \( 1 \leq r < 2^n \). Also, we are assuming that \( 2^n | m - 1 \), so this implies that

\[ 5^n r \equiv 1 \mod 2^n \]

This equation has the unique solution in \( \mathbb{Z}/2^n \) because \( \gcd(5^n, 2^n) = 1 \). **Case 4:** Write \( m = 2^n r \). Then, since \( m < 10^n \), \( 1 \leq r < 5^n \). Also, we are assuming that \( 5^n | m - 1 \), so this implies that

\[ 2^n r \equiv 1 \mod 5^n \]

This equation has the unique solution in \( \mathbb{Z}/5^n \) because \( \gcd(5^n, 2^n) = 1 \). Thus, for each case, there is exactly one non-negative integer of \( n \) digits satisfying the required property. Note that this proof shows us how to find these integers. For \( n = 5 \), these integers are:

**Case 1:** 00000, **Case 2:** 00001, **Case 3:** 90625, **Case 4:** 09376

**Exercise 4: (**) 4 points**

1. If \( m \) is an odd integer, show that \( m^2 \equiv 1 \mod (8) \).
2. Let \( m \) be an odd integer. Show \( m^{2^n} \equiv 1 \mod (2^{n+2}) \) for all positive natural numbers \( n \).

**Solution:**
1. In the light of the Division Algorithm, there exists an integer $k$ such that $$m = 2k + 1$$

We calculate $$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(2k+1) + 1$$

Observing $k(k+1)$ is even, since $k$ (respectively, $k+1$) is even when $k$ is even (respectively, odd), we deduce

$$8|4k(k+1)+1$$

hence

$$m^2 \equiv 1 \mod (8)$$

2. We will prove the result using induction on $n$. The base case $n = 1$ is covered by part 1. above. Assume $k \geq 1$ and suppose $$m^{2^k} \equiv 1 \mod (2^{k+2})$$

By definition, there exists an integer $q$ such that $$m^{2^k} = 1 + 2^{k+2}q$$

Therefore,

$$m^{2^{k+1}} = m^{2^k \times 2} = (m^{2^k})^2 = (1 + 2^{k+2}q)^2 = 1 + 2 \times 2^{k+2}q + (2^{k+2}q)^2 = 1 + 2^{k+3}q + 2^{2(k+2)}q^2 = 1 + 2^{k+3}(q + 2^{k-1}q^2)$$

Since $k \geq 1$, the expression $q + 2^{k-1}q^2$ is an integer, hence the preceding calculation allows us to conclude

$$m^{2^{k+1}} \equiv 1 \mod 2^{k+3}$$

(PMI) allows us to conclude

$$m^{2^n} \equiv 1 \mod 2^{n+2}$$

for all positive integers $n$.

Exercise 5: (⋆) 4 points
Show that no perfect square has $2$, $3$, $7$, or $8$ as its last digit. (Hint: work modulo 10).

Solution:

If $$m = a_k...a_1a_0$$
is the decimal expansion of \( m \) then
\[
    m - a_0 = a_{k} \ldots a_1 0 = 10 \cdot a_k \cdot \ldots \cdot a_1
\]

This shows \( m \) is congruent modulo 10 to its last digit. Since an integer \( m \) is congruent modulo 10 to its last digit \( a_0 \), the fact congruence behaves well with respect to multiplication yields
\[
    m^2 \equiv a_0^2 \pmod{10}
\]

In particular, the last digit of \( m^2 \) is congruent to that of \( a_0^2 \). Using the following table, the last digit of \( a_0^2 \), \( 0 \leq a_0 \leq 9 \) cannot equal 2, 3, 7, or 8; the preceding discussion allows us to conclude that none of the listed numbers can occur as the last digit of a perfect square.

\[
\begin{array}{cccccccc}
    a_0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
    a_0^2 & 0 & 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 \\
    \text{last digit} & 0 & 1 & 4 & 9 & 6 & 5 & 6 & 9 & 4 & 1 \\
\end{array}
\]

\(^1\)\( (*) = \text{easy, } (**) = \text{medium, } (***) = \text{challenge} \)