Math 312: Selected Solutions to Homework 4

Problem 1

(a) Find a complete system of residues mod 7 consisting entirely of primes.
(b) Find a complete system of residues mod 5 consisting entirely of perfect cubes.

1a. We claim that \( \{3, 2, 5, 29, 13, 7, 11\} \) is a complete residue system modulo 7 consisting of primes. Indeed, reducing the list modulo 7 gives \( \{3, 2, 5, 1, 6, 0, 4\} \) which includes exactly once all the numbers in \([0, 6]\), so any integer \( m \) is congruent modulo 7 to exactly one of them.

1b. We claim that \( \{125, 216, 512, 8, 64\} \) is a complete residue system modulo 5 consisting of perfect cubes. Indeed, reducing the list modulo 5 gives \( \{125, 216, 512, 8, 64\} = \{5^3, 6^3, 8^3, 2^3, 4^3\} = \{0, 1, 2, 3, 4\} \) which includes exactly once all the numbers in \([0, 4]\), so any integer \( m \) is congruent modulo 5 to exactly one of them.

Problem 2

Let \( m \in \mathbb{Z}_{>0} \) and let \([r], [s] \in \mathbb{Z}/m\mathbb{Z}\). Prove that multiplication, as defined by

\[
[r] \cdot [s] := [r \cdot s],
\]

is a well-defined operation on \( \mathbb{Z}/m\mathbb{Z} \).

We need to show that the result of the multiplication of congruence classes does not depend on the representatives we choose. Indeed, let \( r' \in [r] \) and \( s' \in [s] \), that is

\[
r' \equiv r \pmod{m} \quad \text{and} \quad s' \equiv s \pmod{m},
\]

hence

\[
r' \cdot s' \equiv r \cdot s \pmod{m} \iff [r \cdot s] = [r' \cdot s'].
\]

We thus have

\[
[r] \cdot [s] := [r \cdot s] = [r' \cdot s'] =: [r'] \cdot [s'],
\]

as desired.
Problem 3

Prove that the inverse of the inverse of \( a \mod m \) is \( a \). More precisely, let \( a^{-1} \) be the inverse of \( a \mod m \) and prove that \((a^{-1})^{-1} \equiv a \mod m\)

By definition of the inverse, \( a^{-1} \) is the integer such that

\[
a \cdot a^{-1} \equiv a^{-1} \cdot a \equiv 1 \mod m.
\]

Similarly, by definition

\[
(a^{-1}) \cdot (a^{-1})^{-1} \equiv (a^{-1})^{-1} \cdot (a^{-1})^{-1} \equiv 1 \mod m.
\]

Multiplying the above congruence by \( a \), we obtain

\[
 a \cdot (a^{-1}) \cdot (a^{-1})^{-1} \equiv a \cdot 1 \mod m.
\]

\[
(a \cdot (a^{-1})) \cdot (a^{-1})^{-1} \equiv a \cdot 1 \mod m.
\]

\[
(1) \cdot (a^{-1})^{-1} \equiv a \mod m. \quad \text{since } a \cdot a^{-1} \equiv 1 \mod m
\]

\[
(a^{-1})^{-1} \equiv a \mod m
\]

as required.

Problem 4

Find all least non-negative incongruent solutions of \( 623x \equiv 511 \pmod{679} \).

We first use Euclidean Algorithm to compute \((623, 679)\). We have

\[
679 = 623 \cdot 1 + 56, \quad 623 = 56 \cdot 11 + 7, \quad 56 = 7 \cdot 8
\]

so, \((623, 679) = 7\). We now apply back substitution

\[
7 = 623 - 56 \cdot 11 = 623 - (679 - 623) \cdot 11 = 12 \cdot 623 - 11 \cdot 679
\]

which means that \( 623 \cdot 12 \equiv 7 \pmod{679} \) and multiplying this congruence by \( 511/7 = 73 \) leads to

\[
623 \cdot (12 \cdot 73) \equiv 511 \pmod{679} \equiv 623 \cdot 197 \equiv 511 \pmod{679},
\]

showing that \( x_0 = 197 \) is a particular solution to the congruence. We now apply the formula that describes the general solution and obtain

\[
x = x_0 - \frac{m}{d} t = 197 - \frac{679}{7} t = 197 - 97t
\]

where \( t \) satisfies \( 0 \leq t \leq 6 \); this gives the solutions

\[
x \equiv 197, 100, 3, 585, 488, 391, 294 \pmod{679}
\]
Problem 5

Solve the following ancient Indian problem: If eggs are removed from a basket 2, 3, 4, 5 and 6 at a time, there remain respectively, 1, 2, 3, 4 and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?

The problem is equivalent to finding the smallest positive solution $x$ to the system of congruences

$$
\begin{align*}
x &\equiv 1 \pmod{2}, & x &\equiv 2 \pmod{3}, & x &\equiv 4 \pmod{5} \\
x &\equiv 3 \pmod{4}, & x &\equiv 5 \pmod{6}, & x &\equiv 0 \pmod{7}.
\end{align*}
$$

Note that the congruence mod 2 is a special case of the congruence mod 4 and the congruence mod 6 can be obtained from the mod 2 and mod 3. Thus the problem is equivalent to solve the following congruences

$$
\begin{align*}
x &\equiv 0 \pmod{7}, & x &\equiv 2 \equiv -1 \pmod{3} \\
x &\equiv 4 \equiv -1 \pmod{5}, & x &\equiv 3 \equiv -1 \pmod{4}.
\end{align*}
$$

Since 3, 4 and 5 are pairwise coprime by CRT the problem is equivalent to

$$
\begin{align*}
x &\equiv 0 \pmod{7}, & x &\equiv -1 \pmod{60}.
\end{align*}
$$

Thus the least possible number of eggs is the smallest number of the form $x = -1 + 60k$ which also satisfies $x \equiv 0 \pmod{7}$.

Since $60 \equiv 4 \pmod{7}$, the smallest positive integer $k$ satisfying

$$
x \equiv -1 + 4k \equiv 0 \pmod{7}
$$

is $k = 2$. Thus $x = -1 + 60 \cdot 2 = 119$.

Alternative: We apply the CRT formula. We have $b_1 = 0$, $b_2 = -1$, $m_1 = 7$, $m_2 = 60$, $M = 60 \cdot 7 = 420$, $M_1 = 60$ and $M_2 = 7$. The solution is given by

$$
x \equiv b_1M_1y_1 + b_2M_2y_2 \equiv -7y_2 \pmod{420},
$$

where

$$
7y_2 \equiv 1 \pmod{60}.
$$

From Problem 2 we have $y_2 = 43$, hence $x \equiv -7 \cdot 43 \equiv 119 \pmod{420}$ and we conclude that $x = 119$ is the smallest amount of eggs.