MATH 9
ASSIGNMENT 22: MODULAR ARITHMETIC AND CHINESE REMAINDER THEOREM

APRIL 2, 2022

Congruence classes and modular arithmetic

Recall that congruence mod n relation

$$a \equiv b \mod n \text{ if } a-b \text{ is a multiple of } n$$

Equivalence classes for this relation are called congruence classes. For example, for $n=3$ we have

$$\begin{aligned}
[0] &= \{\dots, -6, -3, 0, 3, 6, \dots\}\\
[1] &= \{\dots, -2, 1, 4, 7, \dots\}\\
[2] &= \{\dots, -1, 2, 5, 8, \dots\}\\
[3] &= \{\dots, -6, -3, 0, 3, 6, \dots\} = [0]
\end{aligned}$$

Set of all equivalence classes mod n is denoted $\mathbb{Z}_n = \mathbb{Z}/(\equiv \mod m)$. There are exactly n congruence classes: $[0]$, $[1]$, $\dots$, $[n-1]$ (because $[n]=[0]$); thus, $\mathbb{Z}_n$ is a finite set with n elements. For example, for $n=3$, we have

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

One can define addition and multiplication in $\mathbb{Z}_n$ in the usual way:

$$\begin{aligned}
[a]+[b] &= [a+b]\\
[a]\cdot[b] &= [ab]
\end{aligned}$$

(note that one needs to check that this definition does not depend on the choice of representatives a, b in each equivalence class – we discussed this.) So defined addition and multiplication satisfy all the usual rules: associativity, commutativity, distributivity (we skip discussion of this). Note, however, that in general it is impossible to divide: for example, $[2][3]=[0]$ in $\mathbb{Z}_6$, but one can not divide both sides by $[3]$ to get $[2]=[0]$.

Inverses

We say that a congruence class $[a] \in \mathbb{Z}_n$ is invertible if there exists a congruence class $[b] \in \mathbb{Z}_n$ such that $[a][b]=1$. For example, $[3]$ is invertible mod 10 because $[3][7]=[3\cdot 7]=[21]=[1]$.

We had the following theorem:

Theorem. *A congruence class $[a] \in \mathbb{Z}_n$ is invertible if and only if $\gcd(a,n)=1$*

For example, $[7]$ is invertible in $\mathbb{Z}_{15}$ (namely, $[7]\cdot[13]=[91]=[1]$), but $[6]$ is not invertible.

To find inverse of $[a] \in \mathbb{Z}_n$, we need to solve equation $ax+ny=1$ (which can be done using Euclid's algorithm); then $ax \equiv 1 \mod n$, so $[a]^{-1}=[x]$.

Chinese Remainder Theorem

Theorem. *Let m, n be relatively prime. Then for any k, l, the system of congruences*

$$\begin{aligned}
x &\equiv k \mod m\\
x &\equiv l \mod n
\end{aligned}$$

has a solution, and any two solutions differ by a multiple of mn.

Proof of this theorem was discussed in class.

A reformulation of this theorem is as follows. Consider the cartesian product $\mathbb{Z}_m \times \mathbb{Z}_n$. This also has addition and multiplication: $(a_1, b_1)+(a_2, b_2)=(a_1+a_2, b_1+b_2)$, and similarly for multiplication.

Theorem. *Let m, n be relatively prime. Then one has a bijection $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ so that addition, multiplication match.*

For example, we have a bijection $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. In other words: if we know the remainder of a number number mod 6, we can compute this number mod 2 and mod 3. Conversely, if we know remainders upon division of a number by 2 and by 3, we can uniquely recover the remainder upon division of this number by 6.

Here is an example showing how one can solve such a system explicitly. Consider the system

$$x \equiv 2 \mod 7$$
$$x \equiv 4 \mod 11$$

From the first equation, we get $x = 7t + 2$. Substituting it in the second equation, we get

$$7t + 2 \equiv 4 \mod 11$$
$$7t \equiv 2 \mod 11$$

To solve this, let us multiply both sides by inverse of [7] mod 11. Using Euclids's algorithm (or guess and check), we find $2 \cdot 11 - 3 \cdot 7 = 1$, so

$$-3 \cdot 7 \equiv 1 \mod 11$$
$$[7]^{-1} = [-3] = [8]$$

Thus, to solve $7t \equiv 2 \mod 11$, we need to multiply with sides by $[7]^{-1} = [8]$, which gives $t \equiv 2 \cdot 8 \equiv 5 \mod 11$. Therefore, original equation has a solution $x = 7 \cdot 5 + 2 = 37$.

Homework

1. Solve the following equations.
   (a) $5x + 3 \equiv 7 \mod 11$
   (b) $4x = 17 \mod 31$

2. Find all solutions of the system

$$x \equiv 5 \mod 13$$
$$x \equiv 9 \mod 12$$

3. (a) Write all invertible elements of $\mathbb{Z}_7$. How many of them are there? For each of them, find the inverse.
   (b) An order of an $[a] \in \mathbb{Z}_n$ is the smallest power k such that $[a]^k = [1]$. For example, order of $[3] \in \mathbb{Z}_{10}$ is 4, because

$$[3]^2 = [9], \qquad [3]^3 = [7], \qquad [3]^4 = [7] \cdot [3] = [21] = [1]$$

   For each invertible element of $\mathbb{Z}_7$, find its order.
   (c) Is there an invertible element $[a]$ in $\mathbb{Z}_7$ such that all other elements are powers of $[a]$?

4. Answer the questions of the previous problem, replacing $\mathbb{Z}_7$ by $\mathbb{Z}_{11}$.

5. (a) Compute the remainder upon division of 4^{2003} by 7.
   (b) Compute the remainder upon division of 4^{2003} by 11.
   (c) Use Chinese Remainder theorem to compute the remainder upon division of 4^{2003} by 77.

6. Find the remainder upon division of 19^{14} by 70.

7. Find the smallest positive integer number such that when divided by 2, 3, 5 it gives remainders 1, 2, 4 respectively, and in addition, it is divisible by 7. [hint: what can you say about number $n + 1$?]

8. Consider the sequence defined by the formulas

$$a_1 = a_2 = a_3 = 1,$$
$$a_k = a_{k-1} + a_{k-2} + a_{k-3} \quad \text{for } k \geq 4$$

   Find $a_{2015} \mod 3$; $a_{2015} \mod 12$.