MATH 415

Modern Algebra I

Lecture 38:
Chinese remainder theorem.

Chinese Remainder Theorem

Theorem Let $n, m \geq 2$ be relatively prime integers and a, b be any integers. Then the system

$$\begin{cases} x \equiv a \bmod n, \\ x \equiv b \bmod m \end{cases}$$

of congruences has a solution. Moreover, this solution is unique modulo nm.

Proof: Since $\gcd(n, m) = 1$, we have $sn + tm = 1$ for some integers s, t. Let $c = bsn + atm$. Then

$$c = bsn + a(1 - sn) = a + (b - a)sn \equiv a \pmod{n},$$
$$c = b(1 - tm) + atm = b + (a - b)tm \equiv b \pmod{m}.$$

Therefore c is a solution. Also, any element of $[c]_{nm}$ is a solution. Conversely, if x is a solution, then $n|(x - c)$ and $m|(x - c)$, which implies that $nm|(x - c)$, i.e., $x \in [c]_{nm}$.

Problem. Solve simultaneous congruences $\begin{cases} x \equiv 3 \bmod 12, \\ x \equiv 2 \bmod 29. \end{cases}$

The moduli 12 and 29 are coprime. First we use the Euclidean algorithm (in matrix form) to represent 1 as an integral linear combination of 12 and 29:

$$\left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & 29 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 12 \\ -2 & 1 & 5 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -2 & 1 & 5 \end{array}\right)$$
$$\to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -12 & 5 & 1 \end{array}\right) \to \left(\begin{array}{cc|c} 29 & -12 & 0 \\ -12 & 5 & 1 \end{array}\right).$$

From the 2nd row of the last matrix, $(-12) \cdot 12 + 5 \cdot 29 = 1$. Let $x_1 = 5 \cdot 29 = 145$, $x_2 = (-12) \cdot 12 = -144$. Then

$$\begin{cases} x_1 \equiv 1 \bmod 12, \\ x_1 \equiv 0 \bmod 29. \end{cases} \qquad \begin{cases} x_2 \equiv 0 \bmod 12, \\ x_2 \equiv 1 \bmod 29. \end{cases}$$

It follows that one solution is $x = 3x_1 + 2x_2 = 147$. The other solutions form the congruence class of 147 modulo $12 \cdot 29 = 348$.

Problem. Solve a system of congruences $\begin{cases} x \equiv 3 \bmod 12, \\ x \equiv 2 \bmod 10. \end{cases}$

The system has no solutions. Indeed, any solution of the first congruence must be an odd number while any solution of the second congruence must be an even number.

Problem. Solve a system of congruences $\begin{cases} x \equiv 6 \bmod 12, \\ x \equiv 2 \bmod 10. \end{cases}$

The general solution of the first congruence is $x = 6 + 12y$, where y is an arbitrary integer. Substituting this into the second congruence, we obtain $6 + 12y \equiv 2 \bmod 10 \iff 12y \equiv -4 \bmod 10 \iff 6y \equiv -2 \bmod 5 \iff y \equiv 3 \bmod 5$. Thus $y = 3 + 5k$, where k is an arbitrary integer. Then $x = 6 + 12y = 6 + 12(3 + 5k) = 42 + 60k$ or, equivalently, $x \equiv 42 \bmod 60$.

Note that the solution is unique modulo 60, which is the least common multiple of 12 and 10.

Problem. Solve a system of congruences

$$\begin{cases} 2x \equiv 3 \bmod 15, \\ x \equiv 2 \bmod 31. \end{cases}$$

We begin with solving the first linear congruence. Since $\gcd(2, 15) = 1$, all solutions form a single congruence class modulo 15. Namely, x is a solution if $[x]_{15} = [2]_{15}^{-1}[3]_{15}$. We find that $[2]_{15}^{-1} = [8]_{15}$. Hence $[x]_{15} = [8]_{15}[3]_{15} = [24]_{15} = [9]_{15}$. Equivalently, $x \equiv 9 \bmod 15$.

Now the original system is reduced to

$$\begin{cases} x \equiv 9 \bmod 15, \\ x \equiv 2 \bmod 31. \end{cases}$$

Next we represent 1 as an integral linear combination of 15 and 31: $1 = (-2) \cdot 15 + 31$. It follows that one solution to the system is $x = 2 \cdot (-2) \cdot 15 + 9 \cdot 31 = 219$. All solutions form the congruence class of 219 modulo $15 \cdot 31 = 465$.

Chinese Remainder Theorem (revisited)

For any integer $n \geq 2$ we have a homomorphism of rings $h_n : \mathbb{Z} \to \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ given by $h(x) = [x]_n$ for all $x \in \mathbb{Z}$. The kernel of h_n is $\mathrm{Ker}(h_n) = n\mathbb{Z}$.

Now for every pair of integers $m, n \geq 2$ we can define a homomorphism $h_{m,n} : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $h_{m,n}(x) = (h_m(x), h_n(x)) = ([x]_m, [x]_n)$ for all $x \in \mathbb{Z}$. The kernel of $h_{m,n}$ is $\mathrm{Ker}(h_{m,n}) = \mathrm{Ker}(h_m) \cap \mathrm{Ker}(h_n) = m\mathbb{Z} \cap n\mathbb{Z}$ $= k\mathbb{Z}$, where $k = \mathrm{lcm}(m, n)$.

Now assume that m and n are coprime, $\gcd(m, n) = 1$. Then $\mathrm{lcm}(m, n) = mn$. By the Fundamental Theorem on Homomorphisms, the ring $\mathbb{Z}/\mathrm{Ker}(h_{m,n}) = \mathbb{Z}/(mn)\mathbb{Z} = \mathbb{Z}_{mn}$ is isomorphic to the image $h_{n,m}(\mathbb{Z})$. Observe that the rings $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same number of elements. Therefore $h_{n,m}(\mathbb{Z}) = \mathbb{Z}_m \times \mathbb{Z}_n$. In particular, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as rings.

The latter fact is essentially a reformulation of the Chinese Remainder Theorem in more sophisticated terms.

Chinese Remainder Theorem (generalized)

Theorem Let $n_1, n_2, \dots, n_k \geq 2$ be pairwise coprime integers and $a_1, a_2, \dots, a_k$ be any integers. Then the system of congruences

$$\begin{cases} x \equiv a_1 \bmod n_1, \\ x \equiv a_2 \bmod n_2, \\ \dots\dots\dots \\ x \equiv a_k \bmod n_k \end{cases}$$

has a solution which is unique modulo $n_1 n_2 \dots n_k$.

Idea of the proof: The theorem is proved by induction on k. The base case $k = 1$ is trivial. The induction step uses the usual Chinese Remainder Theorem.

Problem. Solve simultaneous congruences

$$\begin{cases} x \equiv 1 \bmod 3, \\ x \equiv 2 \bmod 4, \\ x \equiv 3 \bmod 5. \end{cases}$$

First we solve the first two congruences. Let $x_1 = 4$, $x_2 = -3$. Then $x_1 \equiv 1 \bmod 3$, $x_1 \equiv 0 \bmod 4$ and $x_2 \equiv 0 \bmod 3$, $x_2 \equiv 1 \bmod 4$. It follows that $x_1 + 2x_2 = -2$ is a solution. The general solution is $x \equiv -2 \bmod 12$.

Now it remains to solve the system

$$\begin{cases} x \equiv -2 \bmod 12, \\ x \equiv 3 \bmod 5. \end{cases}$$

We need to represent 1 as an integral linear combination of 12 and 5: $1 = (-2) \cdot 12 + 5 \cdot 5$. Then a particular solution is $x = 3 \cdot (-2) \cdot 12 + (-2) \cdot 5 \cdot 5 = -122$. The general solution is $x \equiv -122 \bmod 60$, which is the same as $x \equiv -2 \bmod 60$.