6. Linear Congruences

Let $m \in \mathbb{N}$ and $f(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{Z}[x]$, $a_r \neq 0$. An integer $a \in \mathbb{Z}$ is a solution of the polynomial congruence

$$f(x) \equiv 0 \pmod{m} \quad \ldots \quad (*)$$

if

$$f(a) \equiv 0 \pmod{m}.$$

If $a \equiv b \pmod{m}$ and $f(a) \equiv 0 \pmod{m}$, then $f(b) \equiv 0 \pmod{m}$. We do not consider a and b as different solutions. We wish to find all solutions for $(*)$ in $\{0, 1, \ldots, m-1\}$ or equivalently, in any complete residue system $\{r_1, \ldots, r_m\}$ mod m.

Ex: (i) $4x \equiv 7 \pmod 8$ has no solutions.
(because $4x-7$, being odd, is not a multiple of 8).

(ii) $x^2 \equiv 1 \pmod 8$ has exactly 4 solutions; namely $1, 3, 5, 7 \pmod 8$

(6.2) If $(a,m)=1$, then $ax \equiv b \pmod m$ has a <u>unique</u> solution.

Proof. We may assume that $b \in \{1, 2, \ldots, m\}$. Since $(a,m)=1$, $\{1, 2, \ldots, m\}$ and $\{a, 2a, \ldots, am\}$ mod m are both complete residue systems mod m. So, there is a <u>unique</u> element $r \in \{1, 2, \ldots, m\}$ such that $ar \equiv b \pmod m$. $\square$

(6.2)(i) If $(a,m) = d$, then the linear congruence

$$ax \equiv b \pmod{m} \quad \cdots \quad (2)$$

has a solution if, and only if, $\cancel{d|m}$ $d|b$.

(ii) If (2) has a solution t, then it has exactly d solutions:

$$A = \left\{t,\ t+\frac{m}{d},\ t+2\frac{m}{d},\ \ldots,\ t+(d-1)\frac{m}{d}\right\},$$

where t is the unique solution of

$$\frac{a}{d}x = \frac{b}{d} \left(\bmod \frac{m}{d}\right) \quad \cdots \quad (3).$$

Proof. (i) Let e be a solution of (2). Then, $ae - b = mt$ for some $t \in \mathbb{Z}$. Since $d|a$ and $d|m$, $d \mid ae - mt = b$.

Conversely, if $d|b$, then $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ and there is a unique solution t for $\frac{a}{d}x \equiv \frac{b}{d} \bmod \left(\frac{m}{d}\right)$.

But t is a solution of (2) also.

(ii). Every solution of (3) is a solution of (2).

- The $\underline{d}$ elements of A are all solutions of (3) and so are solutions of (2).
- No two elements of A are congruent mod m.

Proof: $t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m}$ for $0 \le r, s \le d-1$

$\Leftrightarrow m \mid \frac{m}{d}(r-s) \Leftrightarrow d \mid r-s \Leftrightarrow r = s$ (since $0 \le |r-s| < d$)

- $y \in \mathbb{Z}$ such that $y \pmod{m}$ is a solution of (2), then $y \equiv y_0 \pmod{m}$ for some $y_0 \in A$.

Proof: $ay \equiv b \pmod{m} \Rightarrow ay \equiv at \pmod{m}$

$\Rightarrow y \equiv t \pmod{\frac{m}{d}}$ (since $d = (a, m)$)

$\Rightarrow y = t + k\frac{m}{d}$ for some $k \in \mathbb{Z}$.

But $k \equiv r \pmod{d}$ for some r, $0 \le r < d$.

So, $k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m}$ and $y = t + r\frac{m}{d} \pmod{m}$.

This completes the proof of (ii). □

(6.3) Simultaneous linear congruences: Chinese remainder theorem.

In this section, we answer questions like the existance of an integer which leaves a reminder 2, 3, 2 when divided by 3, 5, 7, respectively.

This question was posed by Sun-Tsu (I st century) and also by the Greek mathematician Nicomachus (circa, 100 AD).

- Formally, we consider a system of linear congruences:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}\right\} \quad (*)$$

and try to find all integers x which satisfy each of these congruences.

1) Such a system need not have any solutions: there is no integer x such that both

$$x \equiv 3 \pmod 2 \quad \text{and} \quad 3x \equiv 0 \pmod 4$$

because the first congruence requires x to be odd and the other requires x to be even.

2). We assume $\gcd(m_i, m_j) = 1$ for all i, j, $i \neq j$,

3) To ensure that each linear congruence in (*) has a solution, we assume that $d_i = (a_i, m_i)$ divides b_i, $i = 1, \dots, r$.

4) By dividing the k^{th} equation in (*) by d_i, $i = 1, \dots, r$, we obtain a new system of congruences

$$\left.\begin{aligned} a_1' x &\equiv b_1' \pmod{n_1} \\ a_2' x &\equiv b_2' \pmod{n_2} \\ &\vdots \\ a_r' x &\equiv b_r' \pmod{n_r} \end{aligned}\right\} (**)$$

For all i, j, $1 \leq i \neq j \leq r$, $(n_i, n_j) = 1$ and $(a_i', n_i) = 1$.

where $n_i = m_i / d_i$.

Since $(a_i, n_i) = 1$, there exists an integer b_i such that $a_i b_i \equiv 1 \pmod{n_i}$, $i = 1, \dots, r$.

Multiplying the i^{th} equation in $(**)$ by b_i for each $i = 1, \dots, r$, we are reduced to finding the solutions in the following

Theorem (Chinese remainder theorem)

Let $n_1, \dots, n_r$ be pairwise relatively prime integers; i.e., $\gcd(n_i, n_j) = 1$ for $1 \leq i \neq j \leq r$. Let $b_1, \dots, b_r$ be arbitrary integers. Then, the system on linear congruences

$$\left.\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_r \pmod{n_r} \end{aligned}\right\} (***)$$

has a unique solution modulo $(n_1 n_2 \cdots n_r)$.

Proof. (i) Let $N = n_1 \cdots n_r$ and $N_i = N/n_i$, $i = 1, \cdots, r$.
Then, $\gcd(N_i, n_i) = 1$ for each i because $(n_j, n_i) = 1$ for each $j \neq i$ and N_i is the product of all n_j, $j \neq i$.
So N_i has a reciprocal $m_i \pmod{n_i}$; i.e., $m_i N_i \equiv 1 \pmod{n_i}$. Now consider

$$x = b_1 N_1 m_1 + b_2 N_2 m_2 + \cdots + b_r N_r m_r.$$

Then, for each i,

$x = b_i n_i m_i \equiv b_i \pmod{n_i}$, completing the existance of a solution

(ii) We now prove the uniqueness of the solution. If $y \in \mathbb{Z}$ is another solution to each linear congruence in (***), then $x \equiv y \pmod{n_i}$ for each i. Since $(n_i, n_j) = 1$ for all $1 \leq i \neq j \leq r$
$x \equiv y \bmod (n_1 \cdots n_r)$. Thus, any two integers satisfying each linear congruence in (***) are congruent $\bmod (n_1 \cdots n_r)$. $\square$