# 3. Linear congruences

## 3.1 Congruences

**Definition 3.1** Let $m$ be a positive integer. Let $a$ and $b$ be integers. We say that $a$ *is congruent to* $b$ *modulo* $m$ if
$$m \mid (a-b).$$
We write
$$a \equiv b \pmod{m}.$$
If $m \nmid (a-b)$, we write
$$a \not\equiv b \pmod{m}.$$

**Theorem 3.1** Let $m$ be a positive integer.
(i) $a \equiv a \pmod{m}$;
(ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;
(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

*Proof.* (i). We have $a - a = 0$ and $m \mid 0$.

(ii). Since $a \equiv b \pmod{m}$, we have $m \mid (a-b)$, and thus $m \mid -(a-b) = (b-a)$, thereby implying that $b \equiv a \pmod{m}$.

(iii). Since $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, we have $m \mid (a-b)$ and $m \mid (b-c)$, and thus $m \mid \big((a-b)+(b-c)\big) = (a-c)$, thereby implying that $a \equiv c \pmod{m}$. ■

R A relation "$\sim$" between the elements of a set $M$ is an *equivalence* if
(i) $a \sim a$ (*reflexivity*);
(ii) If $a \sim b$, then $b \sim a$ (*symmetry*);
(iii) If $a \sim b$ and $b \sim c$, then $a \sim c$ (*transitivity*).
Congruence modulo a fixed $m$ is an equivalence relation.

**Theorem 3.2** We have
(i) $a \equiv b \pmod{m}$ if and only if $a - b \equiv 0 \pmod{m}$;

(ii) If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m},$$
$$a_1 a_2 \equiv b_1 b_2 \pmod{m};$$

(iii) If $a \equiv b \pmod{m}$, then for any positive integer $k$,

$$a^k \equiv b^k \pmod{m};$$

(iv) If $f(x_1, x_2, \ldots)$ is a multivariate polynomial with integer coefficients, and $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, ..., then

$$f(a_1, a_2, \ldots) \equiv f(b_1, b_2, \ldots) \pmod{m}.$$

*Proof.* Exercise. ■

**Theorem 3.3** If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then

$$a \equiv b \pmod{[m,n]}.$$

R If $(m,n) = 1$, then by Theorem 2.10, we have $[m,n] = \frac{mn}{(m,n)} = mn$. Thus in this case $a \equiv b \pmod{mn}$.

*Proof.* Since $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, we have $m \mid (a-b)$ and $n \mid (a-b)$. Thus, $a-b$ is a common multiple of $m$ and $n$, and thus a multiple of $[m,n]$. ■

Note that if $ka \equiv ka' \pmod{m}$, it is *not* always true that $a \equiv a' \pmod{m}$.

**Example 3.1** We have $10 \times 1 \equiv 10 \times 4 \pmod{15}$, but $1 \not\equiv 4 \pmod{15}$. However, it is true that $1 \equiv 4 \pmod{3}$ where $3 = \frac{15}{(10,15)} = \frac{15}{5}$.

**Theorem 3.4** If $(k,m) = d$, then $ka \equiv ka' \pmod{m}$ if and only if $a \equiv a' \pmod{\frac{m}{d}}$.

*Proof.* We write $k = k_1 d$ and $m = m_1 d$ so that $(k_1, m_1) = 1$. Thus,

$$\frac{ka - ka'}{m} = \frac{k(a-a')}{m} = \frac{k_1(a-a')}{m_1}.$$

Since $(k_1, m_1) = 1$, the left-hand side is an integer if and only if $m_1 \mid (a - a')$, namely, $a \equiv a' \pmod{m_1}$ while we also note that $m_1 = \frac{m}{d}$. ■

Now, we can determine in which case one may apply "division" to congruences.

**Corollary 3.5** If $(k,m) = 1$, then $ka \equiv ka' \pmod{m}$ if and only if $a \equiv a' \pmod{m}$.

## 3.2 Residue classes

**Definition 3.2** A set $\{a_1, a_2, \ldots, a_m\}$ is called a *complete residue system modulo $m$*, or a *complete system modulo $m$*, if

(i) $a_i \not\equiv a_j \pmod{m}$ for any $i \neq j$;

(ii) For any integer $a$, there exists an index $i$ such that $a \equiv a_i \pmod{m}$.

**Example 3.2** (i). $\{0,7,2,-3,-8,5\}$ is a complete system modulo 6; (ii). $\{0,1,2,\ldots,n-1\}$ is a complete system modulo $n$.

R Given a set of $m$ integers, to verify whether it forms a complete system modulo $m$, it suffices to check if the $m$ integers are pairwise distinct modulo $m$.

**Theorem 3.6** Let $\{a_1,\ldots,a_m\}$ be a complete system modulo $m$ and let $k$ be an integer with $(k,m)=1$. Then $\{ka_1,\ldots,ka_m\}$ is also a complete system modulo $m$.

*Proof.* (i). Show $ka_i \not\equiv ka_j \pmod{m}$ for $i \neq j$. Otherwise, if $ka_i \equiv ka_j \pmod{m}$, then since $(k,m)=1$, we have $a_i \equiv a_j \pmod{m}$ by Corollary 3.5, yielding to a contradiction to the assumption that $\{a_1,\ldots,a_m\}$ is a complete system modulo $m$.

(ii). Show $a \equiv ka_i \pmod{m}$ for some $i$. Since $(k,m)=1$, we may find integers $k'$ and $m'$ such that $kk'+mm'=1$ by Theorem 2.5, and thus $kk' \equiv 1 \pmod{m}$. Choose $i$ such that $a_i \equiv ak' \pmod{m}$. Then $ka_i \equiv k(ak') = a(kk') \equiv a \pmod{m}$. ∎

**Theorem 3.7** Let $m$ and $m'$ be such that $(m,m')=1$. Suppose that $a$ runs through a complete system modulo $m$ and $a'$ runs through a complete system modulo $m'$. Then $a'm+am'$ runs through a complete system modulo $mm'$.

*Proof.* There are $mm'$ numbers $a'm+am'$. Thus, it suffices to verify that they are pairwise distinct modulo $mm'$. Note that if

$$a_1'm+a_1m' \equiv a_2'm+a_2m' \pmod{mm'},$$

then since $(m,m')=1$, it follows from Corollary 3.5 that

$$a_1m' \equiv a_2m' \pmod{m} \qquad \Rightarrow \qquad a_1 \equiv a_2 \pmod{m}$$

and

$$a_1'm \equiv a_2'm \pmod{m'} \qquad \Rightarrow \qquad a_1' \equiv a_2' \pmod{m'}.$$

leading to the same choice of $a'm+am'$ as $a$ runs through a complete system modulo $m$ and $a'$ runs through a complete system modulo $m'$. ∎

## 3.3 Linear congruences

**Theorem 3.8** The linear congruence

$$ax \equiv b \pmod{m} \tag{3.1}$$

is solvable if and only if $(a,m) \mid b$. In this case, there is a unique solution modulo $\frac{m}{(a,m)}$.

*Proof.* The congruence $ax \equiv b \pmod{m}$ is equivalent to $b-ax=my$ for some $y$. That is

$$ax+my=b. \tag{3.2}$$

By Theorem 2.5, it has integer solutions $(x,y)$ if and only if $b$ is a multiple of $(a,m)$.

For the second part, assume that $(x_0,y_0)$ is a solution to (3.2). Then we parametrize its solutions as follows. First, note that

$$ax+my=b=ax_0+my_0.$$

Thus, $a(x-x_0)=m(y_0-y)$, or if we put $d=(a,m)$,

$$\frac{a}{d}(x-x_0)=\frac{m}{d}(y_0-y).$$

Since $(\frac{a}{d},\frac{m}{d})=1$, we have that for $k\in\mathbb{Z}$,

$$\begin{cases} x-x_0=k\cdot\frac{m}{d}, \\ y_0-y=k\cdot\frac{a}{d}, \end{cases} \quad\Rightarrow\quad \begin{cases} x=x_0+k\cdot\frac{m}{d}, \\ y=y_0-k\cdot\frac{a}{d}. \end{cases}$$

Thus, modulo $\frac{m}{d}$, $x$ has only one possibility. ■

Now, our question is how to construct an explicit expression of the solution to $ax\equiv b \pmod{m}$.

**Definition 3.3** Let $a$ and $m$ be such that $(a,m)=1$. We say that $\bar{a}$ is a *modular inverse of $a$ modulo $m$* if

$$a\bar{a}\equiv 1 \pmod{m}.$$

**Theorem 3.9** Let $a$, $b$ and $m$ be such that $d\mid b$ where $d=(a,m)$. Then the solution to $ax\equiv b \pmod{m}$ is given by

$$x\equiv a'\cdot\frac{b}{d} \pmod{\frac{m}{d}},$$

where $a'$ is the modular inverse of $\frac{a}{d}$ modulo $\frac{m}{d}$.

*Proof.* Note that we may rewrite $ax\equiv b \pmod{m}$ as

$$d\cdot\frac{a}{d}x\equiv d\cdot\frac{b}{d} \pmod{m},$$

which is equivalent to

$$\frac{a}{d}x\equiv\frac{b}{d} \pmod{\frac{m}{d}}.$$

by Theorem 3.4 as $(d,m)=d$. Note also that $a'\cdot\frac{a}{d}\equiv 1 \pmod{\frac{m}{d}}$. Thus,

$$x\equiv a'\cdot\frac{b}{d} \pmod{\frac{m}{d}},$$

which is our desired result. ■

■ **Example 3.3** *Solve* $10x\equiv 15 \pmod{35}$: We have $d=(10,35)=5$. Also, $\frac{10}{5}\times 4\equiv 1 \pmod{\frac{35}{5}}$. Thus, $x\equiv 4\times\frac{15}{5}=12 \pmod{\frac{35}{5}}$, that is $x\equiv 5 \pmod{7}$. ■

## 3.4 Chinese remainder theorem

We have seen that linear congruences are essentially equivalent to $x\equiv c \pmod{m}$.

**Theorem 3.10** The system

$$x\equiv c_1 \pmod{m_1}, \tag{3.3a}$$
$$x\equiv c_2 \pmod{m_2}, \tag{3.3b}$$

has a solution if and only if $(m_1,m_2)\mid(c_2-c_1)$. The solution, if it exists, is unique modulo $[m_1,m_2]$.

*Proof.* From (3.3a), we may write $x = m_1 y + c_1$ for some indeterminate $y$. Substituting it into (3.3b), we have

$$m_1 y + c_1 \equiv c_2 \pmod{m_2},$$

or

$$m_1 y \equiv c_2 - c_1 \pmod{m_2}.$$

By Theorem 3.8, it is solvable if and only if $(m_1, m_2) \mid (c_2 - c_1)$. Further, the solution $y$ is unique modulo $\frac{m_2}{(m_1,m_2)}$, and thus the solution $x$ is unique modulo $m_1 \cdot \frac{m_2}{(m_1,m_2)} = [m_1, m_2]$ by Theorem 2.10. ∎

**Corollary 3.11** Let $m_1$ and $m_2$ be such that $(m_1, m_2) = 1$. Then the system in Theorem 3.10 is solvable, and its solution is unique modulo $m_1 m_2$.

In general, we may consider an analogous system with multiple linear congruences. Along this line, we have the *Chinese Remainder Theorem*, which first appears in the writings of Sun Tzu (孙武: 孙子兵法), and was further developed by Qin Jiushao (秦九韶).

**Theorem 3.12 (Chinese Remainder Theorem).** Let $m_1, \ldots, m_r$ be such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system $x \equiv c_i \pmod{m_i}$ for $1 \leq i \leq r$ has a unique solution modulo $m_1 \cdots m_r$.

*Proof.* This result follows by an iterative application of Corollary 3.11. ∎