5. Divisibility and congruences

The concept of congruence relation was introduced by Carl Friederich Gauss (1777-1855).

Def: Let $m \in \mathbb{Z}$, $m > 0$, and $a, b \in \mathbb{Z}$. We say that a is congruent to b modulo m (and write $a \equiv b \pmod{m}$) if $m \mid a-b$.

'$\equiv$' is called a congruence relation and m is called the modulus of the congruence relation.

Ex. If $m = 2$, then $a \equiv b \pmod{2}$ if both a and b are evens; or both a and b are odd.

(5.1) 'congruence mod m' is an equivalence relation on the set $\mathbb{Z}$ of integers ($\forall m \in \mathbb{N}$).

This means: for $a, b, c \in \mathbb{Z}$,

(i) $a \equiv a \pmod{m}$ for all a; (Reflexivity relation)

(ii) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ for all $a, b \in \mathbb{Z}$ (Symmetry);

(iii) $a \equiv b \pmod m$, $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ for all $a, b, c \in \mathbb{Z}$ (transitivity).

Proof - Exercise. □

For $a \in \mathbb{Z}$, the set $\{b \in \mathbb{Z} : a \equiv b \pmod m\} = C_m(a)$ is called the congruence class of $a \bmod m$.

(5.1) Note that: (i) For $x, y \in \mathbb{Z}$, $C_m(x) = C_m(y)$ if and only if $x \in C_m(y)$;

(ii) $\mathbb{Z}$ is a disjoint union of the sets $\{C_m(x) : x \in \mathbb{Z}\}$

(iii) $C_m(x) = \{x + mk : k \in \mathbb{Z}\}$

(iv) $\mathbb{Z} = \bigcup_{i=0}^{m-1} C_m(i)$ (disjoint union).

For $a, b \in \mathbb{Z}$, either $C_m(a) = C_m(b)$ or $C_m(a) \cap C_m(b) = \phi$.

(v) $C_m(0) =: m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$ is a sub-group of $\mathbb{Z}$ with respect to addition.

(vi) Let $\mathbb{Z}_m := \{0, 1, \cdots, m-1\}$ is a (cyclic) group with respect to addition modulo m, i.e., for $r, s \in \mathbb{Z}_m$, $r + s = t$, $t \in \mathbb{Z}_m$ if $r + s \equiv t \pmod{m}$.

(vii) For each $r \in \mathbb{Z}_m$, $C_m(r) = r + m\mathbb{Z}$ is a coset of $m\mathbb{Z}$ in $\mathbb{Z}$.

(viii) $\mathbb{Z}_m$ has exactly one representative from each congruence class modulo m and no two members of $\mathbb{Z}_m$ are congruent modulo m.

(5.2) 'congruence mod m' for $m \in \mathbb{N}$ shares most properties (except that more care should be taken when 'dividing'). We have:

$a \equiv b \pmod m$ and $\alpha \equiv \beta \pmod m$ implies $a\alpha + \alpha\gamma \equiv b\alpha + \beta\gamma \pmod m$

Let $a \equiv b \pmod m$ and $\alpha \equiv \beta \pmod m$. Then:

(i) $ax + \alpha y \equiv bx + \beta y \pmod m$ for all $x, y \in \mathbb{Z}$;

(ii) $a\alpha \equiv b\beta \pmod m$;

(iii) $a^n \equiv b^n \pmod m$ for each $n \in \mathbb{N}$;

(iv) $f(a) \equiv f(b) \pmod m$ for each $f(x) \in \mathbb{Z}[x]$;

(v) $na \equiv nb \pmod m$ for each $n \in \mathbb{Z}$

Proof: (i) follows because $m \mid (a-b)x + (\alpha-\beta)y$.

(ii) follows because $a\alpha - b\beta = a\alpha - b\alpha + b\alpha - b\beta$
$= (a-b)\alpha + (\alpha-\beta)b$.; (v) is clear;

(iii) follows because $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$

(iv) follows from (i), (iv), (v) and (iii). □

(5.3) Structures on $\mathbb{Z}_m := \{0, 1, \cdots, m-1\}$, $m \geq 2$.

There are two binary operations called addition (written '+') and multiplication (written '.') defined as follows: let $r, s \in \mathbb{Z}_m$, $r+s = t$, $r.s = n$, $(t, s \in \mathbb{Z}_m)$ if $r+s \equiv t \pmod m$ and $r.s \equiv n \pmod m$. We have:

(i) $(\mathbb{Z}_m, +)$ is a cyclic abelian group;

(ii) $(\mathbb{Z}_m, +, .)$ is a commutative ring with identity. It is an integral domain if, and only if, m is prima. (*)$_1$

(iii) The only subgroups of $\mathbb{Z}_m$ are the subgroups of the form $k\mathbb{Z}_m$, $k \in \mathbb{Z}_m$. These are also the only ideals of $\mathbb{Z}_m$.

(*)$_1$ If m is a prima, $\mathbb{Z}_m$ furnishes a field.

Recall that: a ring R is said to be an integral domain if: for $r, s \in R$, $rs = 0$ if, and only if, either $r = 0$ or $s = 0$.

A subset A of a commutative integer R is said to be an ideal of R if: (i) A is a subgroup of R; and (ii) for all $r \in R$ and $a \in A$, $ra \in A$.

For ex: for each $s \in R$, $A = Rs = \{rs : r \in R\}$ is an ideal (called a cyclic ideal); $A = \mathbb{Z}$ in $\mathbb{R}$ and $A = \mathbb{Z}[x]$ in $R = \mathbb{R}[x]$ are not ideals.

Proof. Except for the integral domain part of (ii), the rest is left as an excercise.

- If m is not a prime, then $m = rs$, for integer r, s with $1 < r, s < m$. Then, $r \neq 0 \neq s$ (in $\mathbb{Z}_m$), but $rs = 0$. So, $\mathbb{Z}_m$ is not an integral domain.
- If m is a prime, we show first that $\mathbb{Z}_m$ is a field. For this, we have to show that, for each $a \in \mathbb{Z}_m$, $a \neq 0$, there exists $b \in \mathbb{Z}_m$, $b \neq 0$ such that $ab \equiv 1 \pmod m$. This would show

each non zero element of $\mathbb{Z}_m$ has a multiplicative inverse. Since $\mathbb{Z}_m$ is a commutative ring for each m, $\mathbb{Z}_m$ would be a field.

Since $0 \neq a < m$ and m is a prime, $\gcd(a, m)$ is 1 and so, there exists integers x and y such that $ax + my = 1$. Considering this equality in integers modulo m, if $b \in \mathbb{Z}_m$ such that $x \equiv b \pmod{m}$, we see that $ab \equiv 1 \pmod{m}$.

Any field F is an integral domain, because if $a, b \in F$, $ab = 0$ and $a \neq 0$ and $a' \in F$ such that $a'a = aa' = 1$, then $0 = a'ab = a' \times ab = (a'a)b = 1 \times b = b$. On the other hand, if $a = 0$, then $ab = \underline{0 \times b} = (0+0)b = \underline{0 \times b} + 0 \times b$. So, $ab = 0 \times b = 0$. □

Examples: $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are all integral domains. (also $\mathbb{Z}_p[x]$ for p-prime)
For. The ring of 2×2 matrices with entries from real numbers is NOT an integral domain.

(5.4) Complete Residue System (CRM) modulo m, $m \in \mathbb{N}$

Def: It is a set Λ of integers $\{r_1, \cdots, r_m\}$ such that: (i) $r_i \not\equiv r_j \pmod m$ for all $1 \le i \ne j \le m$;

(ii) for each $r \in \mathbb{Z}$, $r \equiv r_i \pmod m$ for a unique i.

Ex: Given m, a complete residue system modulo m is not unique. Here are some examples:

$\{0, 1, \cdots, m-1\}$, $\{1, 2, \cdots, m\}$, $\{1, 2+l_1 m, 3+l_2 m, \cdots, m+l_{m-1} m\}$ for any choice of $l_1, \cdots, l_{m-1} \in \mathbb{Z}$.

5.4.1 Theorem: If $t \in \mathbb{Z}$ with $(t, m) = 1$ and $\{r_1, \cdots, r_m\}$ is CRM mod m, then so is $\{tr_1, \cdots, tr_m\}$.

Proof. It follows because, since $(t, m) = 1$, for $1 \le i, j \le m$

$$tr_i \equiv tr_j \pmod m \iff m \mid (r_i - r_j) \iff r_i \equiv r_j \pmod m$$

$$\iff m \mid t(r_i - r_j) \qquad \iff i = j. \ \square$$

(by $(t, m) = 1$)

Theorem: Let $a, b, d \in \mathbb{Z}$. ~~and $\gcd(a,b) = d$~~.

(i) $a \equiv b \pmod{m}$, $d \mid m$, $d \mid a \Rightarrow d \mid b$.

(ii) $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

(iii) $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ and $(m,n)=1$ $\Rightarrow a \equiv b \pmod{mn}$

Pf: (i) $a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow d \mid a-b \Rightarrow d \mid b$.

(ii) $a \equiv b \pmod{m} \Rightarrow a = b + mt$ for some $t \in \mathbb{Z}$

If $e = (a, m)$, then $e \mid a$, $e \mid m$, so $e \mid b$.

If $f = (b, m)$, $e \mid b$, $e \mid m$, so $e \mid f$.

Reversing the roles of a and b in the above argument, we have $f \mid e$. So, $e = f$.

(iii) Clear from Fundamental Theorem of Arithmetic. □

(5.5) b-ary (b>0) expansion of integers.

Let $b \in \mathbb{N}$. Given $n \in \mathbb{N}$ can be written as

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 b^0, \quad 0 \le a_i < b \quad (*)$$

Ex. $b=10$, $b=2$, $b=p_i$ a prime

Ex: (i) $b=10$, $n=4368 = 4\times10^3 + 3\times10^2 + 6\times10^1 + 8\times10^0$

(ii) $b=2$, $n=105 = 1\times2^6 + 1\times2^5 + 0\times2^4 + 1\times2^3 + 0\times2^2 + 0\times2^1 + 1\times2^0$.

We say that (*) is a b-ary expansion of n and abbreviate as $(a_m a_{m-1} \cdots a_1 a_0)_b = n$. In this notation

Ex(i), $4368 = (4368)_{10}$ and $(105)_{10} = (1101001)_2$.

Ex1: Calculate $5^{110} \pmod{131}$

$5^{110} = 5^{2^6}\cdot 5^{2^5}\cdot 5^{2^3}\cdot 5^{2^2}\cdot 5^2$

Ans. $110 = 2^6 + 2^5 + 2^3 + 2^2 + 2 \equiv (1101110)_2$

$5^2 \equiv 25 \pmod{131}$

$5^4 \equiv 101 \pmod{131}$

$5^8 \equiv 114 \pmod{131}$

$5^{16} \equiv 27 \pmod{131}$

$5^{32} = 74 \pmod{131}$

$5^{64} = 105 \pmod{131}$. So

$5^{110} \equiv 105\times74\times114\times101\times25$

$\equiv 60 \pmod{131}$ □

Ex2: Let $n = a_0 + a_1(10)^1 + \cdots + a_t(10)^t$, $(0 \le a_i \le 9)$

$= (a_t a_{t-1} \cdots a_0)_{10} = a_t a_{t-1} \cdots a_0$.

Thm: i) $n \equiv a_0 - a_1 + \cdots + (-1)^t a_t \pmod{11}$

Pf. because $10 \equiv -1 \bmod 11$, $10^0 \equiv 1 \pmod{11}$,
and more generally, $10^r \equiv (-1)^r \pmod{11}$. □

ii) $n \equiv a_0 + a_1 + \cdots + a_t \pmod 9$. □

Illustration: Let $n = 1571724$. Then

$1+5+7+1+7+2+4 = 27 \equiv 0 \pmod 9$
$4-2+7-1+7-5+1 = 11 \equiv 0 \pmod{11}$ } so $99 \mid n$. □.

Ex3: $1! + 2! + 3! + \cdots + (100)! \equiv 9 \pmod{12}$

Pf. Since $n! \equiv 0 \bmod 12$ for all $n \ge 3$, LHS $= 1! + 2! + 3! \equiv 9 \pmod{12}$. □

Ex4. $F_5 = 2^{2^5} - 1 \equiv 0 \bmod 641$

Pf: $2^{2^3} = 256$; $2^{2^4} \equiv 65,536 \equiv 154 \pmod{641}$

So, $2^{2^5} \equiv (154)^2 \equiv 640 \equiv -1 \pmod{641}$. □

(5.6) Divisibility and Cancellation

(4) If $c \in \mathbb{N}$ and $ac \equiv bc \pmod{m}$ and $d = (c, m)$, then $a \equiv b \pmod{\frac{m}{d}}$.

Proof: $m \mid c(a-b)$. So, $\frac{m}{d} \mid \frac{c}{d}(a-b)$. But $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$
So, $\frac{m}{d} \mid (a-b)$. □

(5.7) Reduced Residue System modulo m, $m \in \mathbb{N}$.

Recall: A complete residue system (CRS) modulo m is a set of m integers $\{r_1, \dots, r_m\} = \Lambda$ such that: (i) each integer is congruent to exactly one r_i (and consequently); (ii) any two elements of the set Λ are incongruent modulo m.

Def. A reduced residue system modulo m (RRS) is a set Ψ of integers $\{s_1, \dots, s_t\}$ of integers satisfying the following properties:

(i) $s_i \equiv s_j \pmod m \iff s_i = s_j$;

(ii) $\gcd(m, s_i) = 1$ for each $i = 1, \dots, t$;

(iii) if $s \in \mathbb{Z}$ and $\gcd(m, s) = 1$, then $s \equiv s_i \pmod m$ for some $i \in \{1, \dots, t\}$ (and, by (i), to a unique i).

Some times it is also called a reduced congruence system.

Ex: 1) $\{1, 3, 5, 7\}$ is a RRS mod 8.

2) If p is a prime, $\{1, 2, \dots, p-1\}$ is a RRS mod p.

Remarks. 1) A complete residue system contains a unique reduced system, but not conversely.

2) Any reduced residue systems $\pmod m$ have the same number of elements. This common number is written as $\varphi(m)$, called the Euler's totient. The function $\varphi : \mathbb{N} \to \mathbb{N}$ taking n to $\varphi(n)$ is called Euler's φ-function.

Prop: If $\{s_1, \cdots, s_{\varphi(m)}\}$ is a reduced residue system mod m and $a \in \mathbb{Z}$ such that $(a, m) = 1$, then $\{as_1, \cdots, as_{\varphi(m)}\}$ is also a reduced residue system mod m.

Pf: Because $as_i \not\equiv as_j \pmod{m}$ for all i, j, $i \neq j$; and $(as_i, m) = 1$ for each i. □

(5.7)(1) **Euler - Fermat Theorem:** If $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$

Pf. Let $\{s_1, \cdots, s_{\varphi(m)}\}$ be a RRS (mod m).
Since $(a, m) = 1$, $\{as_1, \cdots, as_{\varphi(m)}\}$ also a RRS (mod m)
So,

$$s_1 s_2 \cdots s_{\varphi(m)} \equiv (as_1)(as_2) \cdots (as_{\varphi(m)}) \pmod{m}$$

Since $(s_i, m) = 1$, $(s_1 \cdots s_{\varphi(m)}, m) = 1$. So, $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

2) **Cor: (Fermat)** If p is a prime, then $a^{p-1} \equiv 1 \pmod{p}$ for each $a \in \mathbb{Z}$ with $(a, p) = 1$.

Proof. Since $\varphi(p) = p - 1$, (5.7) yields the Corollary. □

3) **Little Fermat theorem**. For $a \in \mathbb{Z}$, and p a prime
$$a^p \equiv a \pmod p$$
Pf: If $p \mid a$, it is clear. (2) implies (2) if $p \nmid a$. □

4) If $a \in \mathbb{Z}$ with $(a, m) = 1$, $ax \equiv b \pmod m$ has a unique solution, namely $x = b\, a^{\varphi(m)-1} \pmod m$

Proof. Since $a^{\varphi(m)} \equiv a \pmod m$, $a^{\varphi(m)-1} \equiv 1 \pmod m$ because $(a, m) = 1$. So,

$x = a^{\varphi(m)-1}(ax) \equiv a^{\varphi(m)-1} b \pmod m$. □

Ex: (1) Solve $5x \equiv 3 \pmod{24}$

Soln: Since $(5, 24) = 1$, $x \equiv 3 \times 5^{\varphi(24)-1} = 3 \times 5^7 \pmod{24}$ is a solution. Since $5^2 \equiv 1 \pmod{24}$, $5^6 \equiv 1 \pmod{24}$

So $x \equiv 15 \pmod{24}$ is the unique solution. □

Ex. 2: Solve $25x \equiv 15 \bmod (120)$ —(*)

Soln: Since $d = (25, 120) = 5$ and $d \mid 15$ the congruence has exactly 5 solutions $\pmod{120}$. By Ex (1), $15 \pmod{24}$ is the solution of $5x \equiv 3 \bmod 24$. The other solutions of (*) are $x = 15 + 24k$, $k = 0, 1, 2, 3, 4$; i.e. $15, 37, 63, 87, 117 \pmod{120}$. □