# Elementary Number Theory

**V.P. Ramesh**
Department of Mathematics
Central University of Tamil Nadu
http://math-analytics.org/vpramesh/

**Definition 1** (Zero divisor)**.** *Let* $n \in \mathbb{N}$ *and* $0 \neq a \in \mathbb{Z}_n$ *is said to be a zero divisor if there exists* $0 \neq b \in \mathbb{Z}_n$ *such that* $ab = 0$.

**Definition 2** (Unit or invertible element)**.** *Let* $n \in \mathbb{N}$ *and* $0 \neq a \in \mathbb{Z}_n$ *is said to be an unit or invertible if there exists* $b \in \mathbb{Z}_n$ *such that* $ab = 1$.

**Lemma 1.** *Let* $n \in \mathbb{N}$ *and* $0 \neq a \in \mathbb{Z}_n$ *be invertible. Then there exists unique* $b \in \mathbb{Z}_n$ *such that* $ab = 1$.

*Proof.* Let $0 \neq a \in \mathbb{Z}_n$. Suppose there exists $b, b' \in \mathbb{Z}_n$ such that $ab = ab' = 1$.

$$\begin{aligned} b &= b.1 \\ &= b.(a.b'), \text{ since } ab' = 1 \\ &= (b.a).b', \text{ by associative property} \\ &= 1.b', \text{ since } ba = 1 \\ b &= b' \end{aligned}$$

□

**Theorem 1.** *Let* $a \in \mathbb{Z}_n$*, then* $a$ *is unit/invertible if and only if* $(a, n) = 1$.

**Theorem 2.** *Let* $a \in \mathbb{Z}_n$*, then* $a$ *is a zero divisor if and only if* $1 < (a, n) < n$.

Now, $\mathbb{Z}_n$ can be partitioned into three sets namely, $\{0\}$, the set of all units/invertible elements, $U_n$ and the set of all zero divisors, $\mathbb{Z}_n \backslash U_n \cup \{0\}$.

Motivated by Theorem 1, $U_n$ can also be defined as the set of all natural numbers which are relatively prime to $n$ and less than $n$. Now,

**Question 1.** *Is* $\cdot : U_n \times U_n \to U_n$ *a function? Is* $U_n$ *an abelian group? Is* $U_n$ *cyclic? Give a minimal counter example while proving.*

**Question 2.** *Is* $+ : U_n \times U_n \to U_n$ *a function?*

**Question 3.** *Is* $\cdot : \mathbb{Z}_n \backslash U_n \times \mathbb{Z}_n \backslash U_n \to \mathbb{Z}_n \backslash U_n$ *a function?*

**Question 4.** *Does there exists a bijection between the following pair of sets?*

1. $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$

2. $\mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$

Let $n \in \mathbb{N}$, from the fundamental theorem of arithmetic $n = p_1^{q_1} p_2^{q_2} \ldots p_k^{q_k}$ for some primes $p_1, p_2, \ldots p_k$ and some natural numbers $q_1, q_2, \ldots q_k$.

3. $\mathbb{Z}_n$ and $\mathbb{Z}_{p_1^{q_1}} \times \mathbb{Z}_{p_2^{q_2}} \cdots \times \mathbb{Z}_{p_k^{q_k}}$

**Theorem 3** (Chinese Remainder theorem)**.**

*1. Let* $n_1, n_2 \in \mathbb{N}$ *such that* $(n_1, n_2) = 1$ *and* $x, a, b \in \mathbb{Z}$. *If*

$$x \equiv a \mod n_1$$
$$x \equiv b \mod n_2.$$

*Then there exists unique* $c \in \mathbb{Z}_{n_1 n_2}$ *such that* $x \equiv c \mod n_1 n_2$.

*2. Let* $n_1, n_2, \ldots, n_k \in \mathbb{N}$ *such that* $(n_i, n_j) = 1, \forall\ i \neq j$ *and* $x, a_1, a_2, \ldots, a_k \in \mathbb{Z}$. *If*

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k \end{aligned}$$

*Then there exists unique* $c \in \mathbb{Z}_{n_1 n_2 \ldots n_k}$ *such that* $x \equiv c \mod n_1 n_2 \ldots n_k$.

*3. Let* $n \in \mathbb{N}$, $n = p_1^{q_1} p_2^{q_2} \ldots p_k^{q_k}$, *where* $p_1, p_2, \ldots p_k$ *are primes and* $q_1, q_2, \ldots q_k$ *are natural numbers and* $x, a_1, a_2, \ldots, a_k \in \mathbb{Z}$. *If*

$$\begin{aligned} x &\equiv a_1 \mod p_1^{q_1} \\ x &\equiv a_2 \mod p_2^{q_2} \\ &\vdots \\ x &\equiv a_k \mod p_k^{q_k} \end{aligned}$$

*Then there exists unique* $c \in \mathbb{Z}_n$ *such that* $x \equiv c \mod n$.

**Experiment 1.** *A person had n number of chocolates. When he distributed the chocolates among 3 people, he was left with 1 chocolate and when distributed among 4 people, he was left with 3 chocolates. How many chocolates the person had?*

*It is equivalent to solve the following system of congruence equations.*

$$x \equiv 1 \mod 3$$

$$x \equiv 2 \mod 4$$

**Solution.**

$$x \equiv 1 \mod 3 \implies x \in \{\dots \textcircled{-2}, 1, 4, 7, \textcircled{10}, 13, 16, 19, \textcircled{22}, \dots\}$$

$$x \equiv 2 \mod 4 \implies x \in \{\dots \textcircled{-2}, 2, 6, \textcircled{10}, 14, 18, \textcircled{22}, \dots\}$$

Therefore the common solution of the above system belongs to $\{\dots -14, -2, 10, 22, \dots\}$. Which can be algebraically written as $x \equiv 10 \mod 12$. The generalisation of this example proves the existence of solution for Chinese remainder theorem. For uniqueness, we prove by contradiction. Suppose $x \equiv 10 \mod 12$ and $x \equiv a \mod 12$ for some $a \in \mathbb{Z}_{12}$, then $10 \equiv a \mod 12$. Hence the uniqueness.

**Experiment 2** (Chinese Remainder Theorem)**.** *The following table represents a bijection $f_1 : \mathbb{Z}_{35} \to \mathbb{Z}_5 \times \mathbb{Z}_7$ such that*

$$f_1(a) = (a \mod 5, a \mod 7)$$

| $\mathbb{Z}_{35}$ | $\to$ | $\mathbb{Z}_5$ | $\times$ | $\mathbb{Z}_7$ | $\mathbb{Z}_{35}$ | $\to$ | $\mathbb{Z}_5$ | $\times$ | $\mathbb{Z}_7$ | $\mathbb{Z}_{35}$ | $\to$ | $\mathbb{Z}_5$ | $\times$ | $\mathbb{Z}_7$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | $\mapsto$ | (0 | | 0) | 12 | $\mapsto$ | (2 | | 5) | 24 | $\mapsto$ | (4 | | 3) |
| 1 | $\mapsto$ | (1 | | 1) | 13 | $\mapsto$ | (3 | | 6) | 25 | $\mapsto$ | (0 | | 4) |
| 2 | $\mapsto$ | (2 | | 2) | 14 | $\mapsto$ | (4 | | 0) | 26 | $\mapsto$ | (1 | | 5) |
| 3 | $\mapsto$ | (3 | | 3) | 15 | $\mapsto$ | (0 | | 1) | 27 | $\mapsto$ | (2 | | 6) |
| 4 | $\mapsto$ | (4 | | 4) | 16 | $\mapsto$ | (1 | | 2) | 28 | $\mapsto$ | (3 | | 0) |
| 5 | $\mapsto$ | (0 | | 5) | 17 | $\mapsto$ | (2 | | 3) | 29 | $\mapsto$ | (4 | | 1) |
| 6 | $\mapsto$ | (1 | | 6) | 18 | $\mapsto$ | (3 | | 4) | 30 | $\mapsto$ | (0 | | 2) |
| 7 | $\mapsto$ | (2 | | 0) | 19 | $\mapsto$ | (4 | | 5) | 31 | $\mapsto$ | (1 | | 3) |
| 8 | $\mapsto$ | (3 | | 1) | 20 | $\mapsto$ | (0 | | 6) | 32 | $\mapsto$ | (2 | | 4) |
| 9 | $\mapsto$ | (4 | | 2) | 21 | $\mapsto$ | (1 | | 0) | 33 | $\mapsto$ | (3 | | 5) |
| 10 | $\mapsto$ | (0 | | 3) | 22 | $\mapsto$ | (2 | | 1) | 34 | $\mapsto$ | (4 | | 6) |
| 11 | $\mapsto$ | (1 | | 4) | 23 | $\mapsto$ | (3 | | 2) | | | | | |

**Experiment 3** (Chinese Remainder Theorem)**.** *Now, since 2 and 4 are not relatively prime, $f_2 : \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_4$ such that*

$$f_2(a) = (a \mod 2, a \mod 4)$$

*is not a bijection which can be seen from the following table.*

| $\mathbb{Z}_8$ | $\to$ | $\mathbb{Z}_2$ | $\times$ | $\mathbb{Z}_4$ |
|---|---|---|---|---|
| 0 | $\mapsto$ | (0 | | 0) |
| 1 | $\mapsto$ | (1 | | 1) |
| 2 | $\mapsto$ | (0 | | 2) |
| 3 | $\mapsto$ | (1 | | 3) |
| 4 | $\mapsto$ | (0 | | 0) |
| 5 | $\mapsto$ | (1 | | 1) |
| 6 | $\mapsto$ | (0 | | 2) |
| 7 | $\mapsto$ | (1 | | 3) |

**Question 5.** *Let $m \mid n$ and $g_1 : \mathbb{Z}_m \to \mathbb{Z}_n$ such that $g_1(a) = a \mod n$. Is $g_1$ a function?*

**Question 6.** *Let $n \mid m$ and $g_2 : \mathbb{Z}_m \to \mathbb{Z}_n$ such that $g_2(a) = a \mod n$. Is $g_2$ a function? If so, is it a bijection?*

**Definition 3** (Euler's totient function)**.** *Let $n \in \mathbb{N}$, Euler's totient function is said to be the number of elements which are relatively prime to $n$ and less than $n$ and it is denoted by $\phi(n)$. In otherwords, $\phi(n) = |U_n|$.*

**Theorem 4.** *Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$. Then there exists a bijection between $U_{mn}$ and $U_m \times U_n$.*

Now, from Theorem 4, we can conclude the following.

**Lemma 2.** *Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. i.e., Euler's totient function is a multiplicative function.*

**Theorem 5** (Fermat's little theorem)**.** *Let $a \in \mathbb{N}$ and $p$ be a prime number. Then $a^p \equiv a \mod p$. Further, if $p \not| a$, then $a^{p-1} \equiv 1 \mod p$.*

**Theorem 6** (Euler's theorem)**.** *Let $a, n \in \mathbb{N}$ such that $(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \mod n$.*

**Note.** Euler's theorem is a generalisation of Fermat's little theorem because, for a prime $p$, $p \not| a \iff (a, p) = 1$; if $(a, n) = 1$, then $n \not| a$ and the converse of the later statement is false. The counter example is $4 \not| 6$ and $(4, 6) = 2$.

**Theorem 7** (Lagrange's theorem)**.** *Let $G$ be a finite group and $H$ be a subgroup of $G$. Then order of $H$ divides order of $G$.*

**Question 7.** Is Lagrange's theorem a generalisation of Euler's theorem?