Number Theory: Notes
by
Anwar Khan

Partial Contents

These are the handwritten notes. We are very thankful to Mr. Anwar Khan for providing these notes.

1. Number Theory ................................................................. 1
2. Divisibility ................................................................. 2
3. Euclids Theorem ........................................................... 15
4. Base of Radix Representation .......................................... 19
5. Common Division .......................................................... 21
6. Method of finding great common divisor ......................... 23
7. G.C.D. more than two integers ....................................... 38
8. Least Common Multiple .................................................. 39
9. The Linear Diophantine Equation ...................................... 45
10. Theory of Primes .......................................................... 54
11. Composite Number ....................................................... 54
12. Prime Divisor .............................................................. 54
13. Congruence ................................................................. 61
14. Complete Residue System ............................................... 85
15. Solutions of the Congruence ............................................ 102
16. Perfect Number ............................................................ 107
17. Reduce residue System ................................................... 123
18. Quadratic residue .......................................................... 191
19. Arithmetic Function ....................................................... 205

Available at www.MathCity.org/msc/notes/
If you have any question, ask at www.facebook.com/MathCity.org

MathCity.org is a non-profit organization, working to promote mathematics in Pakistan. If you have anything (notes, model paper, old paper etc.) to share with other peoples, you can send us to publish on MathCity.org.
For more information visit: www.MathCity.org/participate/
Number Theory

is also called arithmetic. It is a mathematical theory that study the properties and relations of integers and their extension both algebraic and analytic.

Number: This also called a natural number one of the unique sequence of element used for counting a collection of individual. The number of English alphabets is 26.

Divisibility: let $a, b \in \mathbb{Z}$, we say that $a$ divides $b$ if $\exists k \in \mathbb{Z}$ such that $b = ak$. Then $a$ is called divisor or factor of $b$ and $b$ is called multiple of $a$. Symbodically it can be written as $a | b$ and read as $a$ divides $b$. If $a$ does not divides $b$ then we write $a \nmid b$. 
Theorem

i) Prove that $a/0 \neq a \in \mathbb{Z}^+$

Proof: we can write $(a+0)$

$0 = a(0)$ where $0 \in \mathbb{K}$

$\Rightarrow a/0$

Hence proved.

ii) Prove that $a/a \neq a \in \mathbb{Z}^+$

Proof: we can write

$a = a(1)$ where $1 \in \mathbb{Z}^+$

$\Rightarrow a/a$ Hence proved.

iii) If $a/b$ and $c \in \mathbb{K}$ then $a/bc$

Proof: Since $a/b$, therefore $f$ an integer

$a$ such that $b = ac_i$

Multiply both sides by $c$

$c \cdot b = ac \cdot c$

$c \cdot et$

$\Rightarrow a/bc$ Hence proved.
Q \text{ if } a \mid b \text{ then } a \mid bc \\
\text{ Sel: } \text{ if } a \mid b \text{ then } b = ac \implies bc = acc \mid bc = a \mid bc \quad(3)

iv) \text{ if } a \mid b \text{ and } b \mid a \text{ Then Prove that } a = \pm b.

\text{Proof: Since } a \mid b \text{ therefore } f \text{ an integer } \neq 0 \text{ such that} \\
b = ac \quad (0) \\
\text{and} \\
b \mid a \text{ Therefore } f \text{ an integer } c_2 \in \mathbb{Z} \text{ such that} \\
a = bc_2 \quad (2)

\text{Using (0) and (2) we get}

c = (ac_2)c_2 \\
c = ac_{2}^{2} \\
c - ac_{2}^{2} = 0 \\
\iff a(c_{2}^{2} - c_{2}) = 0 \\
\iff a \neq 0 \text{ Therefore } 1 - c_2 = 0 \\
\iff c_{2} = 1 \\
\implies a = c_2 = \pm 1.

\text{Substituting } c_{2} = \pm 1 \text{ in eqn (2) we get} \\
\therefore a = \pm 1 \\
\text{which is the required result.}
\( y \leq 1 \) \& \( \forall x \& a \in \mathbb{Z} \).

**Proof:**

We can write

\[ a = (-1)(-a) \quad \text{where} \quad -a \in \mathbb{Z} \]

\[ \Rightarrow -1 \mid a \]

Similarly, we can write

\[ a = (a)(1) \quad \text{where} \quad a \in \mathbb{Z} \]

\[ \Rightarrow 1 \mid a \quad \text{Hence the result} \]

vi) If \( ab \) and \( b \mid c \) then \( a \mid c \)

**Proof:**

Since \( ab \), therefore \( 3 \) an element \( c \in \mathbb{Z} \) s.t.

\[ b = ac \] \( -1 \)

and \( b \mid c \)

i.e., \( \exists \) an integer \( c_2 \in \mathbb{Z} \) such that

\[ c = bc_2 \] \( -2 \)

Using (1) in (2) we get

\[ c = ac_1c_2 \]

\[ \Rightarrow a \mid c \] which is required result.
vii) If \( a \mid b \) and \( a \mid c \) Then \( a \mid b + c \).

**Proof:**

Since \( a \mid b \)

\[ b = ac_1 \quad (1) \]

and

\[ a \mid c \]

\[ c = ac_2 \quad (2) \]

Multiply \((1)\) by \( n \) and \((2)\) by \( j \) then adding

\[ bx + cy = ac_1x + ac_2y \]

\[ = ac_3 + ac_4 \]

\[ = a(c_3) \]

\[ \Rightarrow a \mid bx + cy. \]

viii) If \( a \mid b_1 + b_2 \) and \( a \mid b_1 \) Then \( a \mid b_2 \).

**Proof:**

Since \( a \mid b_1 + b_2 \) therefore there exist an integer \( c_1 \) s.t.

\[ b_1 + b_2 = ac_1 \quad (1) \]

and

Since \( a \mid b_1 \) therefore exist an integer \( c_2 \) s.t.

\[ b_1 = ac_2 \quad (2) \]
Putting (2) in (1) we get:

\[ b_1 + b_2 = ac_1 \]

\[ \Rightarrow b_2 = ac_1 - b_1 \]

\[ \Rightarrow b_2 = ac_1 - ac_2 \]

\[ = a(c_1 - c_2) \]

\[ b_2 = ac_3 \]

\[ \Rightarrow a \mid b_2 \] which is the required result.

For e.g. \[ a \mid 4 + 6 \]

Then \[ 2 \mid 6 \]

For e.g. \[ 3 \mid 9 + 6 \]

Then \[ 3 \mid 6 \]

For e.g. \[ 5 \mid 15 + 5 \] and \[ 5 \mid 15 \]

Then \[ 5 \mid 5 \]
Theorem: Prove that $a - b \mid a^n - b^n$, for $n \geq 0$.

Proof: We prove it by mathematical induction.

For $n = 0$

$$a - b \mid a^0 - b^0 = 0$$

$$\Rightarrow a - b \mid 0$$

which is true since $a \mid 0$ and $a \in \mathbb{Z}$.

Suppose the statement is true for $n = k$.

So

$$a - b \mid a^k - b^k$$

We now prove that the statement is true for $n = k + 1$. Then

$$a^{k+1} - b^{k+1} = a^k \cdot a - b^k \cdot b + ab^k - ab^k$$

$$a^{k+1} - b^{k+1} = a(a^k - b^k) + b^k(a - b)$$

Since $a - b \mid a^k - b^k$, there

$$a - b \mid a(a^k - b^k)$$

and $a - b \mid b^k(a - b)$

Hence, $a - b \mid a^{k+1} - b^{k+1}$, which is required.

Hence, the statement is true for $n > 0$, as desired.
Theorem (A+2) \( a + b \mid a^n + b^n \) if \( n \) is odd.

Proof: We prove it by mathematical induction.

For \( n = 1 \)

\[ a + b \mid a + b \] is true.

Suppose that the statement is true for \( n = 2k+1 \)

\[ a + b \mid a^{2k+1} + b^{2k+1} \]

We are to show that the statement is true for \( n = 2(k+1) + 1 = 2k+3 \).

Then:

\[ a^{2k+3} + b^{2k+3} = a^{2k+1} + b^{2k+1} \frac{a^2 + b^2}{2} \]

\[ = a^{2k+1} + b^{2k+1} \frac{a^2 - b^2}{2} \]

\[ = a^{2} \left( a^{2k+1} + b^{2k+1} \right) + b^{2k+1} (a^2-b^2) \]

as \( a \mid b \) then \( a \mid b^2 \). Therefore:

\[ a + b \mid a^{2k+1} + b^{2k+1} \]

Then:

\[ a + b \mid a^2 \left( a^{2k+1} + b^{2k+1} \right) - (1) \]
and \( a + b | b^{2n+1} (a+b)(a-b) \) \( \text{(2)} \)

Therefore from (1) \& (2) we have
\[
\begin{align*}
\Rightarrow & a + b | a^2 + b^{2n+1} + b^{2n+1} (a+b)(a-b) \\
= & a + b | a^{2n+2} + b^{2n+2}
\end{align*}
\]

Hence the statement is true for 
\[ n = 2n+3 \quad \text{odd} \]

Hence the given statement is true, \( \forall n \in \mathbb{Z} \)

Q. \( \text{Note:} \quad a + b | a^n - b^n \) if \( n \) is even.

\[ a + b | a^n - b^n \]

Suppose that the statement is true for 
\[ n = 2k \]

\[ a + b | a^{2k} - b^{2k} \] \( \text{(1)} \)

we are to show that the statement is true for 
\[ n = 2(k+1) = 2n+2 \]

\[
\begin{align*}
a^{2n+2} + b^{2n+2} &= a^{2n} \cdot a^2 + b^{2n} b^2 \\
&= a^{2n} \cdot a^{2k} b^2 + b^{2k} (a^{2k} + b^{2k}) \\
&= a^{2n} (a^{2k} - b^{2k}) + b^{2k} (a^{2k} + b^{2k}) \\
&= a^{2n} (a^{2k} - b^{2k}) + b^{2k} (a+b)(a-b)
\end{align*}
\]
As \( a+b \) divides \( a^2 - b^2 \) therefore
\[
a+b \mid a^2 (a-b).
\]
and
\[
a+b \mid b^2 (a+b)(a-b).
\]
From (3) and (4) we have
\[
a+b \mid 2^{2k+2} - 2^{2k+2}.
\]
Hence the statement \( \forall x \in \mathbb{E} \)
\[
\text{mean } +\text{ve even integer}.
\]

\[\text{If } n \text{ is odd then } 8 \mid n^2 - 1.\]

\[\text{Solution:}\]
As \( n \) is odd then we can write \( n = 2k+1 \) where \( k \in \mathbb{Z} \).
Take
\[
m^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1).
\]
Either \( k \) is even or odd.

Case 1: \( k \) is even then \( k = 2k_1 \) putting in eq (1)
\[
m^2 - 1 = 4(2k_1)(2k_1 + 1) = 8k_1(2k_1 + 1)
\]
As \( 8 \mid 8k_1(2k_1+1) \)

There

\[ 8 \mid n^2 - 1 \]

Case II

if \( n \) is odd, then \( n \) is an integer

\[ k = 2k_2 + 1 \]

Putting in equation (1) we get:

\[ n^2 - 1 = 4(2k_2+1)\left(2(2k_2+1)+1\right) \]

\[ = 4(2k_2+1)(4k_2+2) \]

\[ = 8(2k_2+1)(2k_2+1) \]

\[ = 8 \mid n^2 - 1. \]

Hence \( 8 \mid n^2 - 1 \) if \( n \) is odd.

Show that the product of any three consecutive integers is divisible by 6.

Proof: Let \( k, k+1, k+2 \) be three consecutive integers. Then we have to show that

\[ 6 \mid k(k+1)(k+2). \]

For \( n = 1 \):

\[ 6 \mid 1(1+1)(1+2) = 6 \mid 6. \]
Suppose that the statement is true for \( n = k \) i.e.

\[
6/k(k+1)(k+2) \text{.}
\]

we are to show that the statement is true for \( n = k+1 \):

\[
(k+1)(k+2)(k+3) = k(k+1)(k+2) + 3(k+1)(k+2) \quad (1)
\]

Since

\[
6/k(k+1)(k+2) \text{ is true by assumption,}
\]

and for

\[
3(k+1)(k+2) \text{ therefore } k \text{ is integer. There are two possibilities i.e } k
\]

is even or \( k \) is odd. If

\( k \) is even then \( k \) an integer \( k_1 \)

S.t

\[
k = 2k_1 \text{ Then } 3(k+1)(k+2) \text{ becomes}
\]

\[
8(k+1)(k+2) = 3(2k+1)(2k+2) = 6(2k_1 + 1)(k_1 + 1) = 2 \cdot 3(k+1)(k+2)
\]

Secondly if \( k \) is odd then \( k \) an integer \( k_2 \)

such i.e i.e \( k = 2k_2 + 1 \) then \( 3(k+1)(k+2) \)

becomes

\[
3(k+1)(k+2) = 3(2k_2+1)(2k_2+3)
\]
for \( m = 0 \)

\[
14 \left\lfloor \frac{4m+2}{3} + 5 \right\rfloor
\]

\[
= 14/14 \quad \text{(True)}
\]

for \( m = 1 \)

\[
14 \left\lfloor \frac{4m+3}{3} + 5 \right\rfloor
\]

\[
= 14 \left\lfloor 78.9 + 125 \right\rfloor = 14 \times 54 = 756.
\]
Suppose that the statement is true for \( n = k \), i.e.

\[
\frac{14}{3} \cdot 3^k + 5
\]

we are to show that the statement is true for \( n = k+1 \), i.e.

\[
\frac{14}{3} \cdot 3^{k+1} + 5\]

\[
= \frac{14}{3} \cdot 3^k \cdot 3 + 5
\]

\[
= \frac{4k+6}{3} \cdot 3^k + 5
\]

\[
= 3 \cdot 3^k + 5 \cdot 3
\]

\[
= 2^{k+1} \cdot 3^k + 5 \cdot 3
\]

\[
= 2^{k+1} (3^k + 5) + 5 \cdot 3
\]

Since \( \frac{14}{3} \cdot 3^{k+1} + 5 \) then \( \frac{14}{3} \cdot 3^k + 5 \)

and \( \frac{14}{3} \cdot 3^{k+1} + 5 \) then \( \frac{14}{3} \cdot 3^k + 5 \)

So \( \frac{14}{3} \cdot 3^k + 5 \)
\[ \frac{4n+6}{3} + 5 \]

Hence the statement is true for \( n = k + 1 \)

Hence \( \frac{4(n+1)+6}{3} + 5 \) \( \rightarrow \) \( n \in \mathbb{Z} \) i.e. \( n \geq 0 \)

**Theorem (Euclid's Theorem)**

Let \( a, b \in \mathbb{Z} \), \( b > 0 \) there exist unique integer \( q \) and \( r \) such that

\[ a = bq + r, \quad 0 \leq r < b. \]

**Proof:** Let \( a \) be a \( \mathbb{Z} \) such that

\[ a = \{ a - bx \geq 0 \} \text{ where } x \in \mathbb{Z} \]

\[ a \equiv q \quad a - b(-q) \in A. \]

If \( \emptyset \in A \) then 0 is the least element of \( A \).

If \( \emptyset \in A \) then \( A \), being a subset of the integers must have a least element. Let us call it \( x \).

For some \( x = q \in \mathbb{Z} \)

\[ x = a - bq \]
\[ a - b \gamma \geq 0 \]

\[ \implies \lambda \geq 0 \quad ; \quad \lambda = a - b \gamma \]

Now we have to prove that \( \lambda < b \).

Suppose that \( \lambda \geq b \).

\[ \implies \lambda - b \geq 0 \]

\[ = a - b \gamma - b \geq 0 \quad ; \quad \gamma = a - b \gamma \]

\[ = a - b (\gamma + 1) \geq 0 \quad a - b \lambda \]

\[ \implies \lambda - b \leq a \]

\[ \implies \lambda - b < \lambda \quad . \text{This contradiction to the fact that} \lambda \text{is the least}
\]
\[ \text{element of A. Hence our supposition} \lambda \geq b \text{ is wrong. Hence,} \]
\[ \lambda < b \]

\[ \text{So} \quad \alpha \leq \lambda < b \]

\[ \lambda = a - b \gamma \]

\[ \alpha = b \gamma + \alpha \quad \text{where} \quad 0 \leq \alpha < b \]

For uniqueness let \( \alpha = b \gamma_1 + \alpha_1 \) -

also \( \alpha = b \gamma + \alpha \quad 0 \leq \alpha < b \).

\[ \text{So} \quad b \gamma_1 + \alpha_1 = b \gamma + \alpha \]

\[ |b \gamma_1 - b \gamma| = |\alpha - \alpha_1| = 0 \]
$|b^q_1 - b^q_2| = |x - z|$

$0 = |x - z|$

$\Rightarrow z = x$

$\Rightarrow b^q_1 + x = b^q_2 + z \quad 0 \leq z < b$

This implies that expression is unique.

Remarks: (In Euclid's Theorem).

i) \( g \) is divided by \( b \) if \( r = 0 \)

ii) \( g \) is called \( \text{quotient} \) and \( r \) is called \( \text{remainder} \).

iii) If \( r = 0 \) then \( b | g \) and conversely if \( b | g \) then \( r = 0 \).
iv) If \( b = 2 \) then \( n = 0 \) or 1 it means

- Every integer is either of the form
  - \( 2k \) or \( 2k+1 \).

If it is of the form \( 2k+1 \) then it is called an odd integer.

If it is of the form \( 2k \) then it is called an even integer.

**Definition:**

- If \( r \leq 0 \) then \( b/a \) and
- Conversely if \( b/a \) then \( r > 0 \).

**Proof:** By Euclid's Theorem we know that:

\[
2 = 1 \cdot 2 + 0 \quad (1)
\]

Since \( r = 0 \) then from eqn \( 1 \):

\[
\text{eqn } 1 \Rightarrow 2 = 1 \cdot b + r \text{ where } r \in \mathbb{Z}.
\]

Then by definition of divisibility:

\[
2 | b.
\]

Conversely suppose that:

\[
b | a
\]

Then \( a \) an element \( \in \mathbb{Z} \) such that:

\[
a = b \cdot a \quad (2)
\]

Also by Euclid's Theorem

\[
a = b \cdot y + r \quad (3)
\]

From eqn \( 2 \) and \( 3 \):

\[
2y + r = a
\]

\[
r = 0 \quad \text{Hence proved.}
\]
Base or radix representation

Every positive integer can be written as

\[ a = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \]

where \( a_n \geq 0 \) and \( 0 \leq a_i < 10 \).

This is called representation of \( a \) in the scale (base) 10 and 10 is called base or radix. In fact, every finitely integer \( a \geq 1 \)

\[ a \]

where \( i = 1, 2, 3, \ldots, n-1 \). Then \( 0 \leq a_i < 10 \).

\[ \text{Note:} \]

On abbreviated form we write

\[ (a_1 a_2 \cdots a_n)_b \]

for any base \( b \geq 1 \). The base is specified at the right end. If no base is specified, then integer is written in the scale of 10.

\[ \text{Example:} \]

\[ (\alpha \beta)_{10} + (\beta \alpha)_{10} \]

where \( \alpha = \text{10} \) and \( \beta = 11 \).

\[ (\alpha \beta)_{10} + (\beta \alpha)_{10} \]

\[ \Rightarrow (1\alpha 1\beta)_{12} \]

\[ (\begin{array}{c} 10 \end{array})_{12} \]

\[ (\begin{array}{c} 11 \end{array})_{12} \]

\[ (\begin{array}{c} 110 \end{array})_{12} \]

\[ \text{Example:} \]

\[ (1\alpha 9)_{12} \]
\[ a = 10, \quad \beta = 11 \]

(i) \((2 \alpha 34)_{12} \times (\beta 934)_{12}\)

(ii) \((2129)_{12} \times (\beta 370)_{12}\)

\[ (2 \alpha 34)_{12} \times (\beta 934)_{12} \]

\[ (211034)_{12} \]

\[ (934)_{12} \]

11514

86000

21860

7080

\[ 451101014_{12} \]

\[ 45 \beta 014 \quad \text{Ans.} \]

\[ (2129)_{12} \times (\beta 370)_{12} \]

\[ (2129)_{12} \]

\[ (1370)_{12} \]

12873

6383

11163

\[ 119070130_{12} \]

\[ (119070 \times 30)_{12} \quad \text{Ans.} \]
Common Divisors

Let $a, b \in \mathbb{Z}$ then $c \in \mathbb{Z}$ is called common divisor of $a$ and $b$ if $c | a$ and $c | b$.

For e.g. $4, 8 \in \mathbb{Z}$ then $2 \in \mathbb{Z}$ is their G.C.D.

Greatest Common Divisors : (G.C.D).

Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}$ is called G.C.D of $a$ and $b$ if

ii) $d > 0$ (i) $d | a$ and $d | b$.

iii) $c | a$ and $c | b$ then $c | d$.

For $4, 8 \in \mathbb{Z}$ then $4/4 = 4/8$ and $4 > 0$ and $2/4 = 2/8$ also $8/4$.

So $4$ is G.C.D.

For e.g. $(-2, -4)$

$-1, -2, 1, 2$ are $c.d$ of $(-2, -4)$.

Therefore G.C.D = $2$ which is always positive. We denote $G.C.D$ of $a$ and $b$ as $(a, b) = d$ for e.g. $(9, 12) = d$ (4) $(4, 12) = 4$. 
The G.C.D. of \(a\) and \(b\) is unique, where \(a, b \in \mathbb{Z}\).

**Proof:**

Let \(d_1\) and \(d_2\) be the two G.C.D. of \(a\) and \(b\).

\[(a, b) = d_1 - \mathbb{O}\text{ and } (a, b) = d_2 - \mathbb{O}\]

If \(d_1\) is G.C.D. of \(a\) and \(b\), then \(d_2\) being the common divisor of \(a\) and \(b\) divides \(d_1\)

i.e. \(d_2 | d_1\) \(\text{(iii)}\)

Similarly, if \(d_2\) is G.C.D. of \(a\) and \(b\), then we have \(d_1 | d_2\) \(\text{(iv)}\)

From (iii) \& (iv)

\[d_1 = \pm d_2 \text{ if } a | b \text{ and } b | a\]

Then \(a = \pm b\).

\[\Rightarrow d_1 = d_2 \text{ or } d_1 = -d_2\]

\[\Rightarrow d_1 = d_2 \text{ (} : d_1, d_2 > 0\text{)}\]

Hence G.C.D. of \(a\) and \(b\) is unique.
Method of Finding G.C.D.

We suppose \( a > b \) and \( b > 0 \) then by Euclid's theorem there are unique integers \( q_1 \) and \( r_1 \) such that
\[
g = b q_1 + r_1 = 0 \quad 0 \leq r_1 < b.
\]
If \( r_1 = 0 \) then \( b \) is called G.C.D. of \( a \) and \( b \).

If \( r_1 \neq 0 \) then there exist \( q_2 \) and \( r_2 \) such that
\[
b = r_1 q_2 + r_2 = 0 \quad 0 \leq r_2 < r_1.
\]

We repeat this process until we obtained a remainder which is zero. Then
\[
r_{n-2} = r_{n-1} q_n + r_n
\]
\[
r_{n-1} = r_n q_{n+1} = 0 \Rightarrow r_{n+1} = 0
\]

Here we note the following properties.

i) \( r_n > 0 \)

ii) \( r_n \mid a \) and \( r_n \mid b \)

iii) From 1) to 2) of \( e \) \( c_n \) and \( e \).

Then \( c_n \mid a \).

Hence \( d_n \) is G.C.D. of \( a \) and \( b \).

i.e. \( (a,b) = d_n \).
There is (just statement  
proof not included in this) 

of \((a,b) = d\) then \(d\) can be 
determined as the linear combination 
of \(a\) & \(b\) i.e.

\[ d = ax + by \quad \text{where } a, b \in \mathbb{Z}. \]

\[ \text{For e.g. } (4, 8) = 4. \]

Then

\[ 4 = 4(-1) + 8(+1). \]

**Exercise**

Find G.C.D. of \((275, 105)\), 
and express it as linear combination 
of 275 and 105.

\[ a = b \cdot d + r \]

\[
\begin{align*}
275 & = 2 \cdot 105 + 65 \\
105 & = 1 \cdot 65 + 40 \\
65 & = 1 \cdot 40 + 25 \\
40 & = 1 \cdot 25 + 15 \\
25 & = 1 \cdot 15 + 10 \\
15 & = 1 \cdot 10 + 5 \\
10 & = 2 \cdot 5 + 0
\end{align*}
\]

Hence

\[ \text{G.C.D.}(275, 105) = 5 \]

\[ 5 \mid 10 \]
\[ 10 \mid 15 \]
\[ 15 \mid 25 \]
\[ 25 \mid 40 \]
\[ 40 \mid 65 \]
\[ 65 \mid 105 \]
\[ 105 \mid 275 \]
\[ 275 \]
Now for linear combination

\[ 5 = 15 - 1.10 \]
\[ = 15 - (\frac{1}{25} - 1.15) \]
\[ = 15 - \frac{1.25}{25} + 1.15 \]
\[ = 2(25) - 1(25) \]
\[ = 2(40) - 2(25) - 1(25) \]
\[ = 2(40) - 3(25) \]
\[ = 2(40) - 3(65 - 1(40)) \]
\[ = 2(40) - 3(65) + 3(40) \]
\[ = 5(40) - 3(65) \]
\[ = 5(105 - 1.65) - 3(65) \]
\[ = 5(105) - 5(65) - 3(65) \]
\[ = 5(105) - 8(65) \]
\[ = 5(105) - 8(275 - 2(105)) \]
\[ = 5(105) - 8(275) + 16(105) \]
\[ = 21(105) - 8(275) \]
\[ 5 = 105(21) + 275(-8) \]

5 = 275(-8) + 105(21) as required

where \( x = -8 \) and \( y = 21 \).
Find the G.C.D of

\((10672, 4147)\) and express it as linear combination of \(10672, 4147\).

\[
10672 = 2 \cdot 4147 + 2378 \quad 4147 \big| 10672 \big(2\big)
\]

\[
4147 = 1 \cdot 2378 + 1769 \quad 2378 \big| 4147 \big(1\big)
\]

\[
2378 = 1 \cdot 1769 + 609 \quad 1769 \big| 2378 \big(1\big)
\]

\[
1769 = 2 \cdot 609 + 551 \quad 609 \big| 1769 \big(2\big)
\]

\[
609 = 1 \cdot 551 + 58 \quad 551 \big| 609 \big(1\big)
\]

\[
551 = 9 \cdot 58 + 29 \quad 58 \big| 551 \big(1\big)
\]

\[
58 = 2 \cdot 29
\]

So G.C.D of

\[
(10672, 4147) = 29.
\]

Now for linear combination:

\[
29 = 1 \cdot 551 - 9 \cdot 58.
\]

\[
= 1 \cdot 551 - 9 \cdot (609 - 1 \cdot 551)
\]

\[
= 1 \cdot 551 - 9 \cdot 609 + 9 \cdot 551
\]

\[
= 10 \cdot 551 - 9 \cdot 609
\]

\[
= 10 \cdot (1769 - 2 \cdot 609) - 9 \cdot 609
\]
29 = 10(1769) - 20(609) - 9(609)

v = 10(1769) - 29(609).

w = 10(1769) - 29(2378 - 1(1769))

x = 10(1769) - 29(2378) + 29(1769)

y = 29(1769) - 29(2378).

z = 29(4147 - 2378) - 29(2378)

a = 29(4147) - 39(2378) - 29(2378)

b = 29(4147) - 68(2378)

c = 29(4147) - 68(10672 - 4147)

d = 29(4147) - 68(10672) + 136(4147)

e = 08 175(4147) - 68(10672)

29 = 10672(-68) + 4147(175)

Hence the linear combination:

10672(-68) + 4147(175) = 29
Theorem:

If \( (a, b) = 1 \) Then \( (a-b, a+b) = 1 \)

Proof:

\( a \), \( b \) are of \( (a-b, a+b) = d \)

\[ d \mid a-b \quad (1) \]

also\[ d \mid a+b \quad (2) \]

\[ \Rightarrow d \mid a-b+a+b \]

\[ \Rightarrow d \mid 2a \quad (3) \]
If \( (b, c) = 1 \) and \( a \mid c \) then \( (a, b) = 1 \).

Proof:

Since \( b \) and \( c \) are relatively prime, so \( x \) and \( y \) exist such that

\[
bx + cy = 1 \quad \text{(1)}
\]

Also \( a \mid c \) implies that there exists an integer \( c \in \mathbb{Z} \) such that

\[
c = aq \tag{2} \quad \text{(By divisibility definition)}
\]

Substituting \( c = aq \) into (1), we get

\[
bx + aqy = 1
\]

or

\[
box + aqy = 1
\]

\[
box + aqy = 1
\]

This shows that \( (a, b) = 1 \) hence proved.
\textbf{E1:}

\begin{align*}
\text{If } (a, b) &= d \quad \text{Then } (ma, mb) &= md.
\end{align*}

Since \((a, b) = d\).

Then

\begin{align*}
\text{If integers } x, y \in \mathbb{Z} \text{ such that } \\
ax + by &= d, \\
\max + mb &= md - 1
\end{align*}

Suppose that \((ma, mb) = d_1\)

\begin{align*}
\Rightarrow d_1 | ma, & \quad d_1 | mb, \\
\Rightarrow d_1 | \max \text{ and } d_1 | mb.
\end{align*}

\begin{align*}
\Rightarrow d_1 | \max + mb, & \quad \therefore md = \max + mb \\
\Rightarrow d_1 | md. & \quad - (2)
\end{align*}

As

\((a, b) = d, \Rightarrow d | a \text{ and } d | b,\)

\begin{align*}
\Rightarrow md | ma \text{ and } md | mb, & \quad \Rightarrow \text{md is } \# \text{ of } ma \text{ and } mb. \therefore \text{md divides} \\
\Rightarrow \text{md} | d_1 - (2); & \quad (ma, mb) = d
\end{align*}

\text{From (2) & (8)}

\begin{align*}
\text{md} &= \pm d_1 \\
\text{But } d_1 \text{ is a c.0. Then} \therefore \\
\text{md} &= d_1 \\
\text{Hence } (ma, mb) &= d_1 \\
\text{Hence Proved}
\end{align*}
If \((k_1, k_2) = 1\) and \(k_1 | a\) and \(k_2 | a\), then \(k_1 k_2 | a\). 

Since \(k_1 | a\), then \(k_1 | 3, 7\) = 1.

By definition of divisibility, \(3 | a\) and \(7 | a\).

If an integer \(e \in \mathbb{Z}\) such that \((3e)(7) | 21\),

\[a = ek_1 \quad \cdots \quad (1)\]

Also \(k_2 / a \Rightarrow \) an integer \(e_2 \in \mathbb{Z}\) such that

\[a = e_2 k_2 \quad \cdots \quad (2)\]

\((k_1, k_2) = 1\), then \(3, 7 \in \mathbb{Z}\).

\[k_1 x + k_2 y = 1\] 

Multiplying both sides by \(a\) we have

\[a(k_1 x) + a(k_2 y) = a\] 

\[3k_1 x + 7k_2 y = a\] 

From (1) \(k_1 x \in \mathbb{Z}\) and \(k_2 y \in \mathbb{Z}\).

Therefore

\[k_1 x + k_2 y = 1\]

\[k_1 x | a \Rightarrow a \in \mathbb{Z}\] 

\[k_2 y | a \Rightarrow a \in \mathbb{Z}\]

\[a = e(k_1 x + k_2 y)\]

Which is required result.
of $K_1 \mid a$ and $n_2 \mid b$. Then $K_1 \mid ab$.

Since $K_1 \mid a$ therefore there exist an integer $c_1$ such that

$$a = K_1 \cdot c_1 \text{ and}$$

Similarly

$$n_2 \mid b$$

Therefore

$$b = n_2 \cdot c_2 \text{ for some integer } c_2 \in \mathbb{Z} \text{ such that}$$

$$b = K_2 \cdot c_2 \text{ and }$$

Multiply $1$ and $2$

we have

$$ab = K_1 K_2 c_1 c_2 \quad \Rightarrow \quad K_1 \mid ab$$

Therefore $K_1 \mid ab$ and hence the proof.

Since $K_1 \mid ab$ again by definition of divisors,

I am misled to such that

$$ab = K_1 c_3 \quad \text{and also } n_2 \mid ab$$

Therefore $K_1$ an integer $c_1 \in \mathbb{Z}$ such

$$ab = K_1 c_3$$

Available at

www.mathcity.org
Theorem

If \((b, c) = 1\) then \((a, bc) = (a, b)(a, c)\).

Proof:
Let \((a, bc) = d\)
\[d = d_1 \times d_2\]
and \((a, b) = d_1\)
\((a, c) = d_2\).

We will prove that
\[d = d_1 \times d_2\]

Now,
\[(b, c) = 1, (a, b) = d_1\]
\[(a, c) = d_2\].

\[\Rightarrow d_1 \mid a \text{ and } d_1 \mid b\] \hspace{1cm} (9/10 = 1)
\[\text{also } d_2 \mid a \text{ and } d_2 \mid c\] \hspace{1cm} (3/5 = 1)
\[\Rightarrow d_1 \text{ and } d_2 \text{ divide } a\]
\[\text{and } d_2 \text{ divide } c\].

\[\Rightarrow (d_1, d_2) = 1\]
\[\therefore (b, c) = 1\]

As \(d_1 \mid a\) and \(d_1 \mid a\) then \(d_1 \mid a - 1\).

As \(d_1 \mid b\) and \(d_2 \mid c\) \(\Rightarrow d_1 \mid b\) and \(d_2 \mid c\).

Then \(d_1 \mid bc\)
\[\Rightarrow d_2 \mid bc\]
\[\Rightarrow d_2 \mid bc\]
\[\Rightarrow d_2 \mid d\]

From (1), (2), (3)
\[d_2 \mid d\]

Therefore,
\[d_2 \mid d\]
Again as \((a, b) = d_1 \quad \& \quad (a, c) = d_2\)

Then \(f_{x_1, y_1, z_2} \quad \& \quad x_2y_2 \in \mathbb{R}\)
such that.

\[a_1 + b_1 = d_1 \quad \tag{4}\]

\[a_2 + c_2 = d_2 \quad \tag{5}\]

Multiplying eqns (4) \& (5)

\[(a_1 + b_1)(a_2 + c_2) = d_1d_2\]

\[a_2x_1 + a_1x_2 + ac_1y_1 + abx_2y_1 + bc_2y_2 = d_1d_2\]

as \(d_1 \neq 0 \& d_2 \neq 0\)

so \(d_1 = d_1d_2 \quad \tag{6}\)

From (3) \& (6) we have

\[d_1d_2 = \pm d\]

But G.C.D. is always the same. Therefore:

\[d_1d_2 = d\]

\[d = d_1d_2\]

\[\Rightarrow (a, b, c) = (a, b) \cdot (b, c)\]
If \((a, c) = 1\), then \((a, bc) = (a, b)\).

Given \((a, c) = 1\) \&

\[ (a, bc) = d \quad \text{and} \quad (a, b) = d_1 \]

Then we have to prove that \(d = d_1\).

\[ (a, b) = d_1 \]

\[ \Rightarrow \quad d_1 \mid a \quad \text{and} \quad d_1 \mid b \]

\[ \Rightarrow \quad d_1 \mid a \quad \text{and} \quad d_1 \mid b \]

\[ \Rightarrow \quad d_1 \mid b \]

As \((a, c) = 1\), therefore \(a, b, c\) are integers \(x, y, z\), s.t.

\[ ax + by = 1 \]

\[ \Rightarrow \quad ax + by = 1 \quad \Rightarrow \quad abx + bcy = b \]

as \(d \mid a \quad \text{and} \quad d \mid b\)

\[ \Rightarrow \quad d \mid abx + bcy \]

\[ \Rightarrow \quad d \mid b \]

\[ \Rightarrow \quad abm + bcy = b' \]
As $d | a$ and $d | b$,

$d$ is C.D. of $a$ and $b$.

But $(a : b) = d$. Therefore

$d | d_1$ — (2)

From (1) x (2) we have

$d = \pm d_1$

But $d_1$ is $\text{G.C.D.}$ Therefore

$d = d_1

\Rightarrow d_1 = d$

$(a , b , c) = (a , b)$

Which is required result

exercise:

If $a = b \gamma + r$ Then

$(a , b) = (b , r)$

or $(a , b) = d_1$ and

$(b , r) = 1$

Then we have to show that

$d = d_1$

Since

$a = b \gamma + r$ — (1)

$a - b \gamma = r$
As \( d \mid a \) and \( d \mid b \) then \( d \mid a - bq \).

\[
\Rightarrow d \mid (a - bq) = r.
\]

As \( d \mid b \) and \( d \mid r \) 

\[
\Rightarrow d \mid \text{C.D. of } b \text{ and } r.
\]

But \((b, r) = d_1\)

\[
\Rightarrow d \mid d_1 . \quad (2)
\]

Now again as

As \( d_1 \mid b \) and \( d_1 \mid r \), 

\[
\Rightarrow d \mid by + r.
\]

\[
\Rightarrow d \mid a + r = a = by + r.
\]

As \( d \mid a \) and \( d \mid b \)

\[
\Rightarrow d \mid \text{C.D. of } a \text{ and } b.
\]

But \((a, b) = d\)

\[
\Rightarrow d \mid d . \quad (3)
\]

From (2) and (3) we have:

\[
d = \pm d_1.
\]

But \( q \cdot d \) is always positive

\[
d = d_1.
\]

So \((a, b) = (b, r)\) which is required result.
G.C.D of more than two integers

i. \( d \) is called G.C.D of \( a_1, a_2, a_3, \ldots, a_n \) if

\[
d > 0
\]

ii. \( d \mid a_i \) for \( i = 1, 2, 3, \ldots, n \).

iii. If \( \forall i \), \( d \mid a_i \) for \( i = 1, 2, 3, \ldots, n \),

and we write \( a_g \) as

\[
(\underbrace{a_1, a_2, a_3, \ldots, a_n}) = d.
\]

* Method of finding G.C.D for more than two integers.

Let \( a_1, a_2, a_3, \ldots, a_n \) are integers.

\[
(\underbrace{a_1, a_2}) = d_1
\]

\[
(d_1, a_3) = d_2
\]

\[
(d_2, a_4) = d_3
\]

\[
(d_{n-2}, a_n) = d_{n-1}
\]

\[
\Rightarrow d_{n-1} = (a_1, a_2, a_3, \ldots, a_n).
\]
Exercise

(a, b) = d \text{ Then } \left(\frac{a}{d}, \frac{b}{d}\right) = 1

\text{As } (a, b) = d \text{ Then } \exists x, y \in \mathbb{Z} \text{ such that }

ax + by = d

\frac{a}{d} \times x + \frac{b}{d} \times y = 1

\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \text{ where } x, y \in \mathbb{Z}, \text{ which required result.}

Least Common Multiple: (L.C.M)

An integer \(m\) is the L.C.M of \(a\) and \(b\) if

1) \(m > 0\)
2) \(a \mid m \text{ and } b \mid m\)
3) \(a \mid c \text{ and } b \mid c \text{ then } m \mid c\)

L.C.M of \(a\) and \(b\) will be denoted by \(\langle a, b \rangle = m\) or \(L.C.M(a, b) = m\)
Theorem: Show that L.C.M of two number is unique.

Prove that L.C.M of \(a\) and \(b\) is unique.

Proof: Let \(\langle a, b \rangle = m_1\) and \(\langle a, b \rangle = m_2\).

Case I

If \(m_1\) is L.C.M of \(a\) and \(b\), then \(m_2\) being common multiple of \(a\) and \(b\) is divisible by \(m_1\). i.e., \(m_1|m_2\) — (1)

Case II

If \(m_2\) is L.C.M of \(a\) and \(b\), then \(m_1\) being common multiple of \(a\) and \(b\) is divisible by \(m_2\).

i.e., \(m_2|m_1\) — (2)

From (1) \& (2) we have:

\[ m_2 = + m_1 \]

But \(m_1\) is L.C.M. Therefore:

\[ m_2 = m_1 \rightarrow m_1 = m_2 \]

Hence L.C.M of \(a\) \& \(b\) is unique.
Theorem: if \((a, b) = d\), then:

\[
m = \langle a, b \rangle = \frac{|ab|}{d} = \frac{|ab|}{d}
\]

Proof: we prove that \(m = \langle a, b \rangle = \frac{|ab|}{d}\) satisfy all three properties:

1. Since \(d > 0\) and \(|ab| > 0\),

\[
\Rightarrow \frac{|ab|}{d} > 0
\]

2. Since \((a, b) = d\),

\[
\Rightarrow d \mid a \quad \text{and} \quad d \mid b.
\]

Then \(\exists\) an integer \(a_1, a_2 \in \mathbb{Z}\) such that:

\[
a = a_1d \quad (1)
\]

\[
b = a_2d \quad (2)
\]

\[
\frac{|ab|}{d} = \frac{|a_1a_2d^2|}{d}
\]

\[
m = \frac{|a_1a_2d|}{d} \Rightarrow \frac{|ab|}{d} = m
\]

\[
m = \frac{|a_1a_2|}{d} \Rightarrow a_1d = a.
\]

Also:

\[
m = |ab| \Rightarrow \text{by putting } b = a_2d
\]

\[
m = |a_1a_2b| = \frac{|a_1a_2|}{d} = m
\]
\( b \mid m \) \( \Rightarrow \) \( n \)

\( \frac{a}{b} \mid \mathbb{Z} \) Then we are to show that \( m \mid c \).

\[ c = a d_1 \quad \text{(B)} \]

\[ c = b d_2 \quad \text{(C)} \]

\[ c = a d_1 = b d_2 \quad \text{(A)} \]

As \( (a, b) = d \)

\[ d \mid a \text{ and } d \mid b \]

\[ \Rightarrow \exists a_1, a_2 \in \mathbb{Z} \text{ s.t. } a = a_1d \text{ and } b = a_2d \]

Using in (A)

\[ c = a_1d_1 = a_2d_2 \quad \text{(B)} \]

\[ a_1d_1 = a_2d_2 \]

\[ a_1d_1 = a_2d_2 \quad \text{or} \]

\[ a_2d_2 = a_1d_1 \]

\[ \Rightarrow a_1 \mid a_2d_2 \]

\[ \Rightarrow a_1 \mid \text{an integer } = \mathbb{Z} \text{ s.t. } a_2d_2 = a_1d_1 \]
\[ \Rightarrow a_1, d_2 \therefore (a_1, a_2) = 1 \]

\[ \Rightarrow t \in 2 \quad \text{s.t.} \]
\[ d_2 = a_1 t \]

Case (B) becomes:
\[ C = a_2 a_1 t \]
\[ C = a_1 a_2 d t \Rightarrow C = m t \Rightarrow m = \frac{a_1 a_2 d}{C} \quad \text{[Eqn (3)]} \]

Hence all the three conditions are satisfied so i.e. M of
\[ m = \langle a_1, b \rangle = \frac{1}{d} \]

\[ m = \ldots \]
The Linear Diophantine Equation

The equation of the form

\[ ax + by = c \]

where \( a, b, c \in \mathbb{Z} \) is called a Diophantine equation.

For example, \( 7x + 8y = 15 \).

Theorem: \( ax + by = c \), \( a, b, c \in \mathbb{Z} \) has an integral solution if \((a,b) \mid c\).

If \((x_0, y_0)\) is a solution of the equation then solution set is

\[ S = \{ (x_0 + \frac{b}{(a,b)}t, y_0 - \frac{a}{(a,b)}t); t \in \mathbb{Z} \} \]

or

\[ S = \{ (x_0 - \frac{b}{(a,b)}t, y_0 + \frac{a}{(a,b)}t); t \in \mathbb{Z} \} \]

Proof: Suppose that

\[ ax + by = c \]

has integral solution.

Then we have to prove \((a,b) \mid c\).

Let \((a,b) = d\), \( d \mid a \) and \( d \mid b \).
\[ d \div ax \quad \text{and} \quad d \div by \]
\[ d \div ax + by. \]
\[ \Rightarrow d \div c; \quad ax + by = c \]
so \((a, b) \mid c\).

Conversely, if \((a, b) \mid c\) then we have to prove that the equation \(ax + by = c\) has integral solution \((a, b) = d\)
\[ \Rightarrow d \mid a \quad \text{and} \quad d \mid b. \]
\[ \Rightarrow f \quad a_1, b_1 \in \mathbb{Z} \] such that
\[ a = a_1d \quad \text{and} \quad b = b_1d \quad \text{where} \quad (a, b) = 1 \]
as
\[ d \mid c \Rightarrow f \quad c \in \mathbb{Z} \] such that
\[ c = c_1d. \]
Also as \((a, b) = d \Rightarrow f \quad x, y \in \mathbb{Z}\] such that
\[ ax + by = d. \]
Then
\[ 1 \Rightarrow \quad ax_0 + b_0y_0 = c_1d. \]
by putting \(d\)
\[ 1 \Rightarrow \quad ax_0 + b_0y_0 = c. \]
\[ \Rightarrow \quad x = c_1x_0 \quad \text{and} \quad y = c_1y_0. \]
an integral solution of \(ax + by = c\).
This completes the first part of the theorem.

Now suppose \( x_0, y_0 \) and \( x_1, y_1 \) be two solutions of \( ax + by = c \) \( (1,2) \).

=> \( ax_0 + by_0 = c \) \( (1) \)

and \( ax_1 + by_1 = c \) \( (2) \)

Subtracting \( (2) \) from \( (1) \) we get:

\[ a(x_0 - x_1) + b(y_0 - y_1) = 0 \]

\[ \Rightarrow a \text{ and } b \text{ are factors of } (x_0 - x_1) \text{ and } (y_0 - y_1) \]

\[ \Rightarrow (a, b) = (1, b_1) \text{ and } (x_0 - x_1, y_0 - y_1) \]

As \( (a, b_1) = 1 \)

Therefore \( a \mid y_1 - y_0 \)

\[ \Rightarrow \text{ for } t \in \mathbb{Z}, \text{ s.t. } \]

\[ y_1 - y_0 = at \]

\[ y_1 = y_0 + at \]

\[ y_1 = y_0 + \frac{a}{b_1} t \]
Using \( y_1 = y_0 + \frac{a}{c} t \) in eqn (3):

\[
a_1(x_0 - x_1) = b_1(y_0 + a_1t - y_0)
\]

\[
a_1(x_0 - x_1) = b_1a_1t.
\]

\[
x_1 - x_0 = b_1t.
\]

\[
x_1 = x_0 + b_1t.
\]

\[
x_1 = x_0 - \frac{b_1}{a_1}t, \quad b_1 = b_1b_2
\]

For each value of \( t \in \mathbb{Z} \):

\[
a_1x_1 + b_1y_1 = c.
\]

\[
a \left( x_0 - \frac{b_1t}{a} \right) + b \left( y_0 + \frac{a_1t}{a} \right) = c
\]

\[
a x_0 - \frac{ab_1}{a}t + by_0 + \frac{a_1b_2}{a}t = c
\]

\[
a x_0 + by_0 = c.
\]

\( \Rightarrow a x_0 + by_0 = c \)

Hence solution set:

\[
S = \left\{ \left( x_0 - \frac{b_1t}{a}, y_0 + \frac{a_1t}{a} \right) \right\}
\]
En. Find all integral solutions of

\[ 69x + 111y = 9000 \] (1)

\[ (x, y) = (9, 6) \]

Hence, solutions \( y \) exist.

\[ 69x + 111y = 9000 \]
\[ 23x + 37y = 3000 \]

\[ \Rightarrow 23x + (23 + 14)y = 23(130) + 10 \]
\[ \Rightarrow 23x + 28y + 14y = 23(130) = 10 \]
\[ \Rightarrow 23(x + y - 130) + 14y = 10 \]
\[ \Rightarrow x + y = 130 \] (2)

\[ 23x + 14y = 10 \]
\[ (14 + 9)x + 14y = 10 \]
\[ 14(x + y) + 9x = 10 \]

\[ \Rightarrow x + y = 130 \] (2)

\[ 14y + 9x = 10 \]
\[ \Rightarrow (9 + 5)y + 9z = 9 + 1 \]
\[ \Rightarrow 9(y + z - 1) + 5v = 1 \]
\[ \Rightarrow y + z - 1 = v \] (3)
\[ 9w + 5v = 1 \]
\[ (4+5)w + 5v = 1 \]
\[ 5(w+v) + 4w = 1 \]
\[ \text{put } w+v = u \quad (5) \]
\[ 5u + 4w = 1 \]
\[ \Rightarrow u = 1 \quad \text{and } w = -1 \]

From (5)
\[ v = u - w \]
\[ = 1 - (-1) \]
\[ v = 2 \]

Put \( v = 2 \), \( w = -1 \) in eqn (4)
\[ 2 + x - 1 = \frac{1}{1} \]
\[ 2 = -2 \]

Put \( 2 = -2 \), \( v = 2 \) in eqn (3) we have
\[ -2 + y = 2 \]
\[ y = 4 \]

Put \( x = -2 \), \( y = 4 \) in eqn (2) we have
\[ x + 4 - 13 = -2 \]
\[ x = 124 \]
\[ x - 126 = -2 \]
\[ x = 124 \]
\[ x = 124 \]

\[ x = -10 = 124 \]
\[ y = 80 = 4 \]

\[ s = \left\{ \begin{align*}
\begin{aligned}
S &= \int (x_0 - b/4t^2, y_0 + a/4t^2) dt \\
S' &= \int (124 - 87t, 4 + 23t) dt \quad t \in \mathbb{R}^2
\end{aligned}
\end{align*} \right. \]
Find the solution

Set of \( \{ \)

1) \( 28 x - 49 y = 179 \)
2) \( 23 x + 105 y = 11 \)
3) \( 5 x + 6 y = 1 \)

So:

Given linear diophantine equation

is

\( 23 x - 49 y = 179 \)

First we find G.C.D of \( (23, 49) \)

So

\( (23, 49) = 1 \)

Hence

\( 23 \mid 49 \) \( \frac{12}{46} \)

So general solution

\( \frac{\lambda}{3} \) \( \frac{23 \lambda}{17} \)

of the given equation exist

\( \frac{2}{1} \) \( \frac{3}{1} \) \( \frac{1}{1} \)

\( 23 x - 49 y = 179 \)

\( 23 x - (23(2) + 3) y = 23(7) + 18 \)

\( 23 x - 23(2 y) + 3 y - 23(7) = 18 \)

\( 23 (x - 2y - 7) + 3 y = 18 \)

Put

\( x - 2 y - 7 = z \) \( \rightarrow 1 \)

\( 23 z + 3 y = 18 \)

\( (7z + 2) z + 3 y = 3 (6) \)
\[3(7z) + 2z + 3y = 3(6)\]

\[3(7z) + 3(6) = 3(6) + 2z = 0.\]

\[3(7z + y - 6) + 2z = 0.\]

Putting \(7z + y - 6 = u, \quad (2)\)

\[3u + 2z = 0\]

\[\Rightarrow u = -2 \quad \text{and} \quad z = -3.\]

\[u = -2 \quad \text{and} \quad z = -3.\]

Putting these values in equation (2)

\[7(-3) + y - 6 = -2\]

\[-27 + y = -2\]

\[y_0 = y = -2 + 27 = 25\]

Putting \(y = 25, \quad z = -3\) in \(eqn (1)\)

\[x - 2(25) - 7 = -3\]

\[x - 57 = -3\]

\[x_0 = x = 57 - 3\]

\[x_0 = x = 54.\]

Hence the integral solution of given \(y_0\) is \(8.8 = \frac{54}{9} x_0 + \frac{54}{9} t, \quad \frac{dy_0}{dt} = \frac{25 + 23t}{9}.\)
Theorem:

Every composite number has a prime divisor $\leq \sqrt{n}$.

Proof: Since $n$ is composite, it has at least one prime divisor $p$.

Let $n = mp$. If $p > \sqrt{n}$, then $m = np$ shows that

$$m \times n < p$$

we have a divisor $m$ of $n$ less than the least which is contradictory.

Hence $p \leq \sqrt{n}$. 

$\therefore \therefore \therefore$
A positive integer \( p \) is called prime number if it has no divisor \( d \) of \( 1 \leq d < p \).

If \( p \geq 2 \) and \( p > 0 \) then \( p \) is said to be prime number if \( p \) has only divisors \( 1 \) and \( p \).

\[ \text{e.g.:} \ 2, 3, 5, 7, \ldots \]

A number \( m \) which is not prime is called composite number and it can be written as \( m = d_1 \cdot d_2 \) where \( d_1, d_2 \) are and \( 1 < d_1, d_2 < m \), divisors of \( m \).

1 is neither prime nor composite.
2 is only even prime number.

Every integer \( m > 1 \) has prime divisor.

**Proof:** If \( m \) is prime then \( m \) is prime divisor of \( m \).

If \( m \) is composite then we can write \( m = d_1 \cdot d_2 \), \( 1 < d_1, d_2 < m \).
If \( d_1 \) is prime, then \( m \) has prime divisor i.e. \( d_1 \).

If \( d_1 \) is composite, then we can write

\[
d_1 = d_3 d_4, \quad 1 < d_3, d_4 < d_1
\]

Let \( d_B < d_4 \).

If \( d_3 \) is prime, then \( m \) has prime divisor i.e. \( d_3 \).

But if \( d_3 \) is composite, we proceed in the same way already we arrive

\[
1 < d_k, \quad d_k+1 < m
\]

such that \( d_k \) cannot be factored more than \( d_k \) is prime number, and \( m \) has prime divisor.

Note: Every composite number has prime divisor i.e. \( \exists \).

If \( p \) is a prime divisor and \( p \mid d_3 \) then \( p \mid a \) or \( p \mid b \).

Proof: Suppose that \( p \nmid a \).

Since \( p \) is prime, then

\[
(p, a) = 1
\]

\[
\implies \exists x, y \in \mathbb{Z} \text{ such that } px + ay = 1.
\]
\[ p x + a y = 1 \]
\[ p b a + a b y = b \]

As
\[ \implies p | p b a \text{ and } p | a b y \]

\[ \implies p | p b a + a b y \]
\[ \implies p | b \quad : \quad p b a + a b y = b. \]

If \( p \) is a prime number and \( p \mid a b = p_1a_1b_1 \cdots p_k a_k b_k \), then
\[ p | a_i \text{ for some } i = 1, 2, 3, \ldots, k. \]

of \( p \mid p_2p_3 \cdots p_n \) where \( p_i \)s are prime.

Then \( p = p_j \) for some \( j = 1, 2, 3, \ldots, k. \)

(The Fundamental Theorem of Arithmetic)

The Unique Factorization Theorem Statement

Every integer \( n > 1 \) can be expressed as a product of primes and this representation is unique except for the order in which they are written.

P.T.O. for P.O.P.
Proof: we prove the theorem by induction on \( n \).

For \( n = 2 \),

\[ 2 = 2 \text{ (true)} \]

Let us suppose that the statement is true for \( n = 2, 3, 4, \ldots, k \).

Now prove it for \( n = k+1 \).

If \( k+1 \) is prime, then the induction is complete. If \( k+1 \) is composite, then it can be written as \( k+1 = k_1 k_2 \).

Then by induction hypothesis, \( k_1, k_2 \) can be expressed as product of primes. So the induction is complete, and the theorem is true. That is, \( n = p_1 p_2 p_3 \ldots p_k \), where \( p_i \) for \( i = 1, 2, 3, \ldots k \) are primes.

For uniqueness, let \( n = p_1 p_2 p_3 \ldots p_k \), where \( k = 9_1 q_2 q_3 \ldots q_r \), where \( i = 1, 2, 3, \ldots r \).

Then

\[ 9_1 q_2 q_3 \ldots q_r = p_1 p_2 p_3 \ldots p_r \]
Then we cancelled common factors from both sides of (1) we obtained

\[ g_1 g_2 g_3 \cdots = p_1 p_2 p_3 \cdots - p_i \quad (2) \]

Then by result of \( p_1 p_2 p_3 \cdots \) where \( p_i : i = 1, 2, 3, \ldots k \)
are primes then \( P = P_i \) for some \( i = 1, 2, 3, \ldots , k \).

Since \( g_1 / g_2 g_3 \cdots = g_i \)
therefore

\[ g_1 / p_1 p_2 p_3 \cdots = p_i \]

Then by above result.

\[ g_1 = P_i \] where for some \( i = 1, 2, 3, \ldots j \)
which is a contradiction hence this prove the uniqueness theorem.

The number of primes is infinite.

Suppose that the number of prime is finite then there largest prime \( P \) (say) such that

\[ 2, 3, 5, 7, 11, \cdots P \].
Now consider the integer

\[ n = (2 \cdot 3 \cdot 5 \cdot \cdots \cdot P) + 1 \]

(1) If \( n \) is prime, then \( n \) is greater than \( p \), which is not possible.
(2) If \( n \) is composite, then it has a prime divisor which is not in \( 2, 3, 5, \ldots, P \).

Consequently, \( n \) is a prime greater than \( p \), which is again a contradiction.

To show by other way:

\[ f(P) = \begin{cases} 3 & \text{if } P = 2 \\ P + 1 & \text{if } P > 2 \end{cases} \]

If a proper subset is equivalent to the given set (i.e., bijective mapping) is defined between them. Then the given set is infinite.
If \( (b, c) = 1 \) and \( bc \) is a perfect square, then prove that \( b \) and \( c \) are perfect squares.

Let
\[
b = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r},
\]
\[
c = q_1^{b_1} q_2^{b_2} q_3^{b_3} \cdots q_t^{b_t},
\]
be the standard form of \( b \) and \( c \).

Since \( b \) and \( c \) are relatively prime,
\[
(b, c) = 1.
\]

So
\[
g_i = p_i^{2r_i}.
\]

Then
\[
i \in \{1, 2, 3, \ldots, r\}
\]
and
\[
j \in \{1, 2, 3, \ldots, t\}
\]
are even. Then
\[
a_i = 2r_i
\]
and each
\[
b_i = 2q_i.
\]

Then eqn(0) becomes:
\[
bc = (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t})
\]
\[
= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t})
\]
\[
= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t})
\]
Hence \( b \) and \( c \) are perfect squares.

For example, as 36 is a perfect square, \((4, 9) = 1\).
\[
36 = 9 \times 4
\]
\[
= (3)^2 \times (2)^2 = 9 \times 4
\]
are also perfect squares.
Gauss (1777-1855) introduce the concept of congruences.

If $m > 0$ and $a, b, m \in \mathbb{Z}$ we say $a$ is congruent to $b$ modulo $m$ if $m \mid a - b$. Then we write

$a \equiv b \pmod{m}$

We say that $a$ is residue of $b$ and $b$ is residue of $a$.

If $m \mid a - b$ then we say $a$ is incongruence to $b \pmod{m}$

$a \not\equiv b \pmod{m}$

E.g.

$4 \equiv 1 \pmod{3}$

$3 \mid 4 - 1 \quad \therefore 3 \mid 3 \quad \therefore 1 \equiv 1 \pmod{3}$

$3 \mid 4 - 1 \quad \quad \therefore 3 \mid 3 - 1 \quad \therefore 4 \equiv 1 \pmod{3}$

$-1 \equiv -2 \pmod{3}$
The congruence relation in \( \mathbb{Z} \) is an equivalence relation.

**Reflexive:** since \( \forall a \in \mathbb{Z} \),
\[
m | a - a
\]
\[
\Rightarrow a \equiv a \pmod{m}
\]

**Symmetric Property:** if \( a \equiv b \pmod{m} \) then \( b \equiv a \pmod{m} \)
\[
\text{since } a \equiv b \pmod{m}
\]
\[
\Rightarrow m | a - b
\]
\[
\Rightarrow m | -(b - a)
\]
\[
\Rightarrow m | b - a
\]
\[
\Rightarrow b \equiv a \pmod{m}
\]

**Transitive Property:** (for \( a, b, c \in \mathbb{Z} \))
\[
\text{if } a \equiv b \pmod{m} \quad \text{and} \quad b \equiv c \pmod{m}
\]
\[
\Rightarrow a \equiv c \pmod{m}
\]
From (1) & (2)
\[ m \mid a - b \quad \& \quad m \mid b - c \]

\[ \Rightarrow m \mid a - b + b - c \]

\[ \Rightarrow m \mid a - c \]

\[ \Rightarrow a \equiv c \pmod{m} \]

Hence, congruence relation in \( \mathbb{Z} \) is an equivalence relation.

Remark:

1) The integers 0, 1, 2, \ldots, m-1 are incongruent modulo m.
   (For any two integers)
   \[ \exists \text{ } a \neq b \]

\[ a \equiv b \pmod{m} \] if and only if \( a \) and \( b \) have the same remainder after division by \( m \).

\[ \text{Suppose that } a \equiv b \pmod{m} \]

\[ \Rightarrow m \mid a - b \]

\[ \Rightarrow \exists \text{ an integer } q \in \mathbb{Z} \text{ such that } a - b = mq \]

Let \( a = mq_1 + r_1 \quad 0 \leq r_1 < m \)

\[ b = mq_2 + r_2 \quad 0 \leq r_2 < m \]

where \( q_1, q_2, r_1, r_2 \in \mathbb{Z} \).
\[ a - b = m \varphi_1 + \varphi_1 - m \varphi_2 - \varphi_2. \]
\[ q - b = m(\varphi_1 - \varphi_2) + \varphi_1 - \varphi_2. \]
\[ m \varphi = m(\varphi_1 - \varphi_2) + \varphi_1 - \varphi_2. \]
\[ m \varphi - m(\varphi_1 - \varphi_2) = \varphi_1 - \varphi_2 \]

\[ \Rightarrow m \mid \varphi_1 - \varphi_2. \]
\[ \text{but} \quad 0 \leq |\varphi_1 - \varphi_2| < m \quad \text{Then } \varphi \text{ must be equal to zero.} \]
\[ |\varphi_1 - \varphi_2| = 0 \]
\[ \varphi_1 = \varphi_2. \]

Conversely, suppose that \( a \neq b \) have same remainders after division by \( m \).
\[ \text{i.e.} \]
\[ a = m \varphi_1 + \varphi \quad \text{Same remainder} \]
\[ b = m \varphi_2 + \varphi \quad 0 \leq \varphi < m \]

\[ a - b = m(\varphi_1 - \varphi_2) + \varphi - \varphi \]
\[ a - b = m(\varphi_1 - \varphi_2) = m \varphi_3 \text{ where} \]
\[ \Rightarrow m \mid a - b. \]
\[ \Rightarrow a \equiv b \pmod{m}. \]
If \( a \equiv b \pmod{m} \)
and \( c \equiv d \pmod{m} \)

Then (1)
\[ a + c \equiv b + d \pmod{m} \]

2) \( a - c \equiv b - d \pmod{m} \)

3) \( ac \equiv bd \pmod{m} \)

**Proof**

Given that

1) \( m \mid a - b \) (i.e., \((a - b) = km\) for some integer \( k \))
   - Also \( c \equiv d \pmod{m} \)

From 0 and 2,

\[ m \mid a - b + c - d \]

\[ m \mid (a + c) - (b + d) \]

\[ \Rightarrow \quad a + c \equiv b + d \pmod{m} \]

2) \( a \equiv b \pmod{m} \)
   - \( m \mid a - b \) (i.e., \((a - b) = km\) for some integer \( k \))
   - Also \( c \equiv d \pmod{m} \)

From 0 and 2,

\[ m \mid c - d \]
From (2) \( \#2 \)

\[
m \bigg| a - b - (c - d)
\]

\[
\Rightarrow m \bigg| a - c - b + d.
\]

\[
\Rightarrow m \bigg| (a - c) - (b - d)
\]

\[
\Rightarrow a - c \equiv b - d \pmod{m}.
\]

**iii)** \( \text{As } a \equiv b \pmod{m} \)

\[
\Rightarrow m \bigg| a - b \quad \Rightarrow a - b = m\gamma_1
\]

\[
\text{and } e \equiv d \pmod{m} \quad \Rightarrow e = m\gamma_2 + d
\]

\[
\Rightarrow m \bigg| e - d.
\]

\[
\Rightarrow e - d = m\gamma_2 + d - d \quad \Rightarrow e = m\gamma_2 + d - 0 \quad \text{by definition of divisibility}
\]

Multiplying (2) \& (4) we get

\[
ac = (m\gamma_1 + b)(m\gamma_2 + d).
\]

\[
ac = m^2\gamma_1\gamma_2 + m\gamma_1 + m\gamma_2 + bd.
\]

\[
ac - bd = m^2\gamma_1\gamma_2 + m\gamma_1 + m\gamma_2 + bd
\]

\[
\Rightarrow m \bigg| ac - bd.
\]

\[
\Rightarrow ac \equiv bd \pmod{m}.
\]
Then \( a \equiv b \pmod{m} \)

1) \( na \equiv nb \pmod{m} \)

2) \( a^n \equiv b^n \pmod{m} \)

Proof:

Since \( a \equiv b \pmod{m} \)

\[ \implies m \mid a - b. \]

\( \implies \exists \text{ an integer } y \in \mathbb{Z} \text{ such that} \]

\[ a - b = my. \]

\[ na - nb = mny. \]

\( \implies na - nb = mny. \quad n' = y \]

\( \implies m \mid na - nb \]

\( \implies na \equiv nb \pmod{m} \)

2) Since \( a \equiv b \pmod{m} \)

\( \implies m \mid a - b. \)

\( \implies m \mid a^n - b^n. \)

so by induction we have
\[ a = b \pmod{m} \Rightarrow m \mid a - b \]

Hence the statement is true.

Let the statement be true for \( n = k \).
\[ a^k = b^k \pmod{m} \]
\[ \Rightarrow m \mid a^k - b^k \]

Consider
\[ a^{k+1} - b^{k+1} = a^k \cdot a - b^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \]
\[ = m \mid a(a^k - b^k) \text{ by (ii)} \]
\[ m \mid b^k(a - b) \text{ by (i)} \]
\[ m \mid a(a^k - b^k) + b^k(a - b) \]
\[ \Rightarrow m \mid a^{k+1} - b^{k+1} \]
\[ \Rightarrow a^{k+1} = b^{k+1} \pmod{m} \]

Hence \( a^m = b^m \pmod{m} \)

\( \forall n \text{ non-negative integer} \)

\( \text{i.e. } n \in \mathbb{Z}^+ \)
If \( ma \equiv nb \pmod{m} \) and \( (m,n) = d \). Then

\[ a \equiv b \pmod{\frac{m}{d}} \]

**Proof:** Since \( ma \equiv nb \pmod{m} \),

\[ \Rightarrow m | ma - nb \quad \text{(1)} \]

Also

\[ (m,n) = d. \]

\[ \Rightarrow d | m \text{ and } d | n. \]

\[ \Rightarrow \exists q_1, q_2 \in \mathbb{Z} \text{ such that } m = q_1d, \quad m = q_2d \text{ where } (q_1, q_2) = 1 \]

\[ 0 = q_1d | q_2d(a - b) \]

\[ \Rightarrow q_1 | q_2(a - b) \]

\[ \Rightarrow q_1 | a - b \quad \text{since } (q_1, q_2) = 1 \]

\[ a \equiv b \pmod{q_1}. \]

\[ \Rightarrow a \equiv b \pmod{\frac{m}{d}} \text{ since } m = q_1d \]
If \( na \equiv nb \pmod{m} \) and \((m,n) = 1\),
then \( a \equiv b \pmod{m} \).

Proof:

Since \( na \equiv nb \pmod{m} \),
we have \( m \mid na - nb \).

Also,

\[
\left( \frac{m}{n} \right) = \frac{m \times 1}{n} \Rightarrow \text{there exist two integers } y_1, y_2 \text{ such that } m = y_1 \times n \text{ and } n = y_2 \times n.
\]

Then, \( m = y_1 \times n = y_2 \times n \). Then \( q_1 / q_2 \) becomes 

\[
q_1 / q_2.
\]

\[
m \mid n(a - b).
\]

Since \( (m, n) = 1 \), therefore

\[
m \mid a - b \Leftrightarrow \frac{a}{b} \equiv \frac{c}{d} \equiv 1 \Rightarrow \text{ then } a \mid c.
\]

\[
\Rightarrow a \equiv b \pmod{f(m)}.
\]
\[ a \equiv b \pmod{m_1} \]
\[ a \equiv b \pmod{m_2} \text{ and } (m_1, m_2) = 1 \]

Then
\[ a \equiv b \pmod{m_1} \]
\[ m_1 \mid a - b \]
If \( f(x) = C_0 + C_1 x + C_2 x^2 + \ldots + C_n x^n \)
where \( C_i \in \mathbb{Z} \)
and if \( a \equiv b \pmod{m} \)
then
\[ f(a) \equiv f(b) \pmod{m}. \]

Proof: we know that
\[ 1 \equiv 1 \pmod{m}, \]
\[ a \equiv b \pmod{m}, \]
\[ a^2 \equiv b^2 \pmod{m}, \]
\[ a^3 \equiv b^3 \pmod{m}, \]
\[ \vdots \]
\[ a^n \equiv b^n \pmod{m}. \]

Multiplying the congruences by \( C_0, C_1, C_2, \ldots, C_n \) respectively and then adding
\[ C_0 a^0 + C_1 a^1 + C_2 a^2 + \ldots + C_n a^n \equiv C_0 b^0 + C_1 b^1 + C_2 b^2 + \ldots + C_n b^n \pmod{m}, \]
which implies
\[ f(a) \equiv f(b) \pmod{m}. \]
Find the remainder when $f(15)$ is divided by 7 where

$$f(x) = x^4 - 3x^2 + 2x - 1.$$ 

Since

$$15 \equiv 1 \pmod{7},$$

$$\Rightarrow f(15) \equiv f(1) \pmod{7}.$$ 

$$f(1) = 1 - 3(1) + 2 - 1$$

$$f(1) = -1$$

$$-1 \equiv 6 \pmod{7}.$$ 

Hence

$$f(15) \equiv 6 \pmod{7}.$$ 

Hence 6 is remainder $f(x)$ is divided by 7.

Find the remainder when $3^2$ is divided by 8.

As

$$3 \equiv 1 \pmod{8},$$

$$\Rightarrow (3^2)^{10} \equiv (1)^{10} \pmod{8}.$$
Find the remainder.

\( g^1 \) is divided by 51.

\( 8 \) is divided by 127.

\( 565 \) is divided by 127.

\[ \text{As } \quad 7^4 = 4 \pmod{51} \]

\( (7)^2 = (4)^2 \pmod{51} \).

\[ 7^8 = 16 \pmod{51} \]

\[ 7^{10} = 49 \times 16 \pmod{51} \]

\[ 7^{10} = 19 \pmod{51} \]
Find the remainder when $3^6$ is divided by $51$.

As,

\[ 3^6 \equiv 30 \pmod{51} \]

\[ (3^6)^2 \equiv 900 \pmod{51} \]

\[ (3^6)^2 \equiv 11 \pmod{51} \]

Find the remainder when $5^{21}$ is divided by $127$.

\[ 5^6 \equiv 4 \pmod{127} \]

\[ 5^{18} \equiv (4^3) \pmod{127} \]

\[ 5^{18} \equiv 64 \pmod{127} \]

\[ 5^{18} \cdot 5 \equiv 5^3 \cdot 64 \pmod{127} \]

\[ 5^{21} \equiv 8,000 \pmod{127} \]

\[ 5^{21} \equiv 126 \pmod{127} \]
From here $2^{10} - 1$ has the factor 23.

Proof:

Since $2^2 = 4 \pmod{23}$

$(2^2)^5 = (4)^5 \pmod{23}$

$2^{10} = 1024 \pmod{23}$

$2^{10} = 19 \pmod{23}$

$2^{10} = 24 \pmod{23}$

$2^{11} = 24 \pmod{23}$

$2^{11} = 1 \pmod{23}$

$2^{11} = 1 - 1 \pmod{23}$

$2^{11} = 0 \pmod{23}$

Therefore, 23 is a factor of $2^{11} - 1$. 

\[ 23 \mid 2^{11} - 1 \]
$2^{23} - 1$ has the factor $47$.

Since

\[ 2^4 = 2^4 \pmod{47} \]
\[ 2^4 = 16 \pmod{47} \]
\[ (2^4)^5 = (16)^5 \pmod{47} \]
\[ 2^{20} = 6 \pmod{47} \]

\[ 2^3 \cdot 2^{20} = 2^3 \cdot 6 \pmod{47} \]
\[ 2^3 = 48 \pmod{47} \]
\[ 2^3 = 1 \pmod{47} \]

\[ 2^{23} - 1 = 0 \pmod{47} \]

\[ \Rightarrow 47 \mid 2^{23} - 1 \]

\[ \Rightarrow 47 \text{ is the factor } \frac{2^{23}}{2-1} \]
If \( ab = c \, (\text{mod } m) \) and \( b = d \, (\text{mod } m) \), then
\[
ad = c \, (\text{mod } m).
\]

\[\text{Proof:} \quad \text{since } ab = c \, (\text{mod } m), \quad m \not| ab - c \]
\[\Rightarrow \text{there is an integer say } q \in \mathbb{Z} \text{ such that } \]
\[ab - c = m q_1 = 0\]

Also
\[b = d \, (\text{mod } m)\]
\[\Rightarrow m | b - d\]
\[\Rightarrow \text{there is an integer } q_2 \in \mathbb{Z} \text{ such that } \]
\[b - d = q_2 m \]
\[\Rightarrow b = d + m q_2\]

Then
\[\text{equation } 0 \Rightarrow a (d + m q_2) - c = m q_1 \]
\[ad + am q_2 - c = m q_1 \]
\[ad - c = m q_1 - am q_2 \]
\[ad - c = m (q_1 - q_2) \]
\[ad - c = m q_3 \]
\[\Rightarrow m | ad - c \quad \Rightarrow ad = c \, (\text{mod } m)\]
Show that an integer written in the scale of 10 is divisible by 9 if the sum of its digits is divisible by 9.

Proof:

Let

\[ a = (d_n d_{n-1} d_{n-2} \ldots d_1 d_0)_{10} \]

be the integer then:

\[ a = 8n \times 10^n + 8n-1 \times 10^{n-1} + \ldots + 8 \times 10 + 8_0 \]

Since,

\[ 1 \equiv 1 \pmod{9} \]
\[ 10 \equiv 1 \pmod{9} \]
\[ (10)^2 \equiv (1)^2 \pmod{9} \]
\[ 10^2 \equiv 1 \pmod{9} \]
\[ 10^3 \equiv 1 \pmod{9} \]
\[ 10^m \equiv 1 \pmod{9} \]
\[ \begin{align*}
\gamma_n 10^n &\equiv \gamma_n \pmod{9}, \quad (i) \\
\gamma_{n-1} 10^{n-1} &\equiv \gamma_{n-1} \pmod{9}, \quad (ii) \\
\gamma_0 10^0 &\equiv \gamma_0 \pmod{9}, \quad (n+1).
\end{align*} \]

Now, adding all congruences from (i) to \((n+1)\) eps,

\[ \gamma_n 10^n + \gamma_{n-1} 10^{n-1} + \cdots + \gamma_1 10^1 + \gamma_0 \equiv \gamma_n + \gamma_{n-1} + \cdots + \gamma_0 \quad \pmod{9}. \]

\[ \Rightarrow a \equiv \gamma_n + \gamma_{n-1} + \gamma_{n-2} + \cdots + \gamma_1 + \gamma_0 \pmod{9}. \]

\[ \Rightarrow 9 \mid a \quad \text{iff} \quad 9 \mid 1 + \gamma_1 + \gamma_2 + \cdots + \gamma_n. \]

**Theorem:** Show that an integer divisible by 8 if the integer formed by its last three digits is divisible by 8.

**Proof:** Let \( a = (\gamma_n \gamma_{n-1} \gamma_{n-2} \cdots \gamma_1 \gamma_0) \) be the integer, then

\[ a \equiv \gamma_n \times 10^n + \gamma_{n-1} \times 10^{n-1} + \cdots + \gamma_0 \times 10 + \gamma_1 + \gamma_2 + \gamma_3 + \cdots + \gamma_n \pmod{9}. \]
Since
\[ 1 \equiv 1 \pmod{8}, \]
\[ 10 \equiv 2 \pmod{8}, \]
\[ 10^2 \equiv 4 \pmod{8}, \]
\[ 10^3 \equiv (4)^3 \pmod{8} \]
\[ 10^3 \equiv 64 \pmod{8}, \]
\[ 10^3 \equiv 0 \pmod{8}, \]
\[ 10^4 \equiv 0 \pmod{8}, \]
\[ 10^{n-1} \equiv 0 \pmod{8}, \]
\[ 10^n \equiv 0 \pmod{8}. \]

Now
\[ b_n 10^n \equiv 0 \pmod{8} \]
\[ b_{n-1} 10^{n-1} \equiv 0 \pmod{8} \]
\[ b_{n-2} 10^{n-2} \equiv 0 \pmod{8} \]
\[ b_{n-3} 10^{n-3} \equiv 4_b \pmod{8} \]
\[ b_1 10 \equiv 24_a \pmod{8} \]
\[ b_0 \equiv b_0 \pmod{8} \]
Now adding all the congruences from (1) to (2n+1) then:

\[ 3n \cdot 10^n + 8n - 1 \cdot 10^{-1} + \cdots + 2\cdot 10^2 + 910 + 80 \equiv 482 + 281 + 80 \pmod{8} \]

\[ A = 482 + 281 + 80 \pmod{8}. \]

\[ A = 1028 + 1081 + 80 \pmod{8}. \]

\[ A = (28180)_{10} \pmod{8}. \]

Hence \( 8 \mid A \) if and only if \( 8 \mid (28180)_{10} \).
We know that the congruence relation \((\text{mod } m)\) in \(\mathbb{Z}\) is an equivalence relation and hence by the fundamental theorem of equivalence relation. If we partition \(\mathbb{Z}\) into disjoint equivalence classes called congruent classes \((\text{mod } m)\) such that all members of same equivalence class are congruent to each other \((\text{mod } m)\) and two members of distinct classes are incongruent \((\text{mod } m)\). Since every integer is congruent to one of 
\[0, 1, 2, 3, \ldots, m-1 \ (\text{mod } m)\]

Then there are exactly \(m\) congruent classes.

Example:

If \(m = 4\). Then

\[C_0 = \left\{ x \in \mathbb{Z} : x \equiv 0 \ (\text{mod } 4) \right\}\]

\[C_1 = \left\{ x \in \mathbb{Z} : x \equiv 1 \ (\text{mod } 4) \right\}\]

\[C_2 = \left\{ x \in \mathbb{Z} : x \equiv 2 \ (\text{mod } 4) \right\}\]

\[C_3 = \left\{ x \in \mathbb{Z} : x \equiv 3 \ (\text{mod } 4) \right\}\]

For \(i = 0\)

\[C_0 = \{ \ldots, -12, -8, -4, 0, 4, 8, 12, \ldots \}\]

For \(i = 1\)

\[C_1 = \{ \ldots, -11, -7, -3, 1, 5, 9, 13, \ldots \}\]

For \(i = 2\)

\[C_2 = \{ \ldots, -10, -6, -2, 2, 6, 10, 14, \ldots \}\]

For \(i = 3\)

\[C_3 = \{ \ldots, -9, -5, -1, 1, 5, 9, 13, \ldots \}\]
\( C_2 = \{ x \in \mathbb{Z} : x \equiv 2 \pmod{4} \} \)

\( C_2 = \{ \ldots, -10, -6, -2, 2, 6, 10, 14, \ldots \} \)

For \( i = 3 \),

\( C_3 = \{ x \in \mathbb{Z} : x \equiv 3 \pmod{4} \} \)

\( C_3 = \{ \ldots, -9, -5, -1, 3, 7, 11, 15, \ldots \} \)

**Note:** Number of equivalence classes are equal to modulo.

\[ \bigcup_{i=0}^{3} C_i = \left\{ 0, \pm 4, \pm 8, \pm 12 \right\} \bigcup \left\{ \ldots, -7, -3, 1, 5, 9, 13, \ldots \right\} \]

\[ \bigcup \left\{ \ldots, -10, -6, -2, 2, 6, 10, 14, \ldots \right\} \]

\[ \bigcup \left\{ \ldots, -9, -5, -1, 3, 7, 11, 15, \ldots \right\} \]

\[ = \mathbb{Z} \] (set of integers).
(C.R.S).

A set $A$ is Complete Residue System $(\text{mod } m)$ if $A$ satisfies the following properties:

1) $A$ has $m$ elements.

2) If $x_i, x_j \in A$ and $i \neq j$ then $x_i \equiv x_j \ (\text{mod } m)$.  

A set $A$ is C.R.S if any integer $a$ is congruent to one of the following elements, i.e. $0, 1, 2, \ldots, m-1$ $(\text{mod } m)$, i.e. for $a \in \mathbb{Z}$,

$$a_i \equiv m-1 \ (\text{mod } m)$$

where $i = 0, 1, 2, 3, \ldots, m-1$. 
For \( E_1 \)

\[ A = \{ 0, 1, 2, 3, 4 \} \]

\[ C. R. S \ (\text{mod} \ 5) \]

\[ A \text{ has } 5 \text{ elements} \]

\[ \forall \text{ for any } a, y \in A \]

\[ a \neq y \ (\text{mod} \ 5) \]

Available at

www.mathcity.org
If \( \{ x_0, x_1, x_2, \ldots, x_{m-1} \} \) is a C.R.S. of \( \text{mod } m \) then for any \( a, b, c \in \mathbb{Z} \)

with \( (a, m) = 1 \) then

\[
A = \{ ax_0 + bx_1, ax_1 + bx_2, \ldots, ax_{m-1} + bx_0 \}
\]

in C.R.S. \( \text{mod } m \).

Proof: As

\[
A = \{ ax_0 + bx_1, ax_1 + bx_2, \ldots, ax_{m-1} + bx_0 \}
\]

Clearly \( A \) has \( m^2 \) elements.

Let \( a_i + b \) and \( a_j + b \in A \) where \( i \neq j \).

So

\[
a_i + b = a_j + b \pmod{m}
\]

\[
= a_i = a_j \pmod{m}.
\]

\[
= x_i = x_j \pmod{m}, \quad (a, m) = 1
\]

which is contradiction as \( x_i \) and \( x_j \) are members of C.R.S.

Hence our supposition is wrong and any two members of \( A \) are

congruence under \( \text{mod } m \).

Consequently \( A \) is complete

Residue System.
If \( \{x_0, x_1, x_2, \ldots, x_{m-1}\} \) is C.R.S. (mod \( m \)) and \( \{y_0, y_1, y_2, \ldots, y_{n-1}\} \) is C.R.S. (mod \( n \)) where \( (m, n) = 1 \), then:

\[
A = \{nx_i + my_j, \ i = 0, 1, \ldots, m-1, \ j = 0, 1, \ldots, n-1\}
\]

is C.R.S. of (mod \( mn \)).

**Proof.** As

\[
A = \{nx_i + my_j, \ i = 0, 1, \ldots, m-1, \ j = 0, 1, \ldots, n-1\}
\]

Clearly \( A \) has \( mn \) elements.

Now let \( nx_i + my_j, \ n x_l + m y_k \) where \( i \neq l \) or \( j \neq k \).

\[
x_i + m y_j \equiv x_l + m y_k \pmod{mn}.
\]

\[
\Rightarrow n(x_i - x_l) \equiv m(y_j - y_k) \pmod{mn}.
\]

\[
\Rightarrow n(x_i - x_l) + m(y_j - y_k) \equiv 0 \pmod{mn}.
\]

\[
\Rightarrow n(x_i - x_l) + m(y_j - y_k) \equiv 0 \pmod{m}.
\]

\[
\Rightarrow x_i - x_l \equiv y_j - y_k \pmod{m}.
\]

\[
\Rightarrow m(y_j - y_k) \equiv m(x_l - x_i) \pmod{mn}.
\]

\[
\Rightarrow y_j - y_k \equiv x_l - x_i \pmod{mn}.
\]
\[ a \Rightarrow m (x_i - x_l) \equiv 0 \pmod{m} \]
\[ \Rightarrow m (y_i - y_k) \equiv 0 \pmod{n} \]
\[ \Rightarrow x_i - x_l \equiv 0 \pmod{m} \]
\[ \Rightarrow y_i - y_k \equiv 0 \pmod{n} \]
\[ \Rightarrow (m, n) = 1 \]
\[ \Rightarrow x_i \equiv x_l \pmod{m} \]
\[ \Rightarrow y_i \equiv y_k \pmod{n} \]

which is contradiction as \( x_i \)'s and \( y_i \)'s are members of complete residue systems.

Hence our supposition is wrong, and any two members \( A \) and \( A' \) are congruent \( \pmod{mn} \). That is \( A' \) is \( C.R.S. \).

**Ex.**

\[ \{0, 1, 2, 3\} \quad \{0, 1, 2, 3\} \]

are \( C.R.S. \) and \( \pmod{3} \)

Then \( m = 3, n = 4 \)

\[ A = \{ m x_i + m y_i : (=3) \} \quad m-1 \{ 0, 1, 2, 3 \} \]

\[ A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\} \]

or

\[ A = \{0, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 17\} \]
we are to show that
\[ A \equiv 0 \mod{12}. \]
Since \( A \) has 12 elements
and for any \( x, y \in A \):
\[ x \neq y \mod{12}. \]
Hence \( A \) is complete
residue system \( \mod{12} \).

An arithmetical function which associates
with every integer \( \leq m \), the number of positive integers less than or equal to \( m \)
and prime to \( m \), is called Euler's function
and is denoted by \( \phi(m) \).
\[
\begin{align*}
\phi(1) &= 1 \\
\phi(2) &= 1 \\
\phi(3) &= 2 \\
\phi(4) &= 2 \sqrt{2} \\
\phi(5) &= 4 \\
\phi(6) &= 2 \cdot 3
\end{align*}
\]
\[ \phi(n) = n - 1 \]

Note: If \( m \) is prime then \( \phi(m) = m - 1 \).
\[
\begin{align*}
\phi(8) &= 3 \\
\phi(9) &= 6(1 - \frac{1}{2})(1 - \frac{1}{3}) \\
\phi(16) &= 2
\end{align*}
\]
\( \phi(m) = m - 1 \) if \( m \) is prime.

Proof: Suppose \( m \) is prime, then all the \( m \) integers less than \( m \) are relatively prime to \( m \).

\[ \Rightarrow \phi(m) = m - 1 \] There are \( m - 1 \) the integers which are relatively prime to \( m \).

Conversely let \( \phi(m) = m - 1 \)

i.e. there are \( m - 1 \) the integers which are relatively prime to \( m \), which is only possible if \( m \) is prime.

For e.g. \( \phi(5) = 4 \), \( 5 \) is prime.

If \( \phi(m) \neq m - 1 \) \( m \) is not prime. Then consider \( \phi(\alpha) \) where \( \alpha \) is prime.

Then there are exactly \( \alpha \) integers not exceeding \( \alpha \) out of which \( \alpha - 1 \) are not prime to \( \alpha \).

Then

\[ \phi(m) = \alpha - 1 \]

for e.g. \( 8 = 2^3 \), \( 2^3 - 2^2 = \phi(8) = 2^3 - 2^1 = 8 - 4 = 4 \).
\[ p_n^{-1} P \left( \frac{n}{p_n} \right) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n \]

Then

\[ p_0 \alpha \] is zero of \( q(x) \) having coefficients are algebraic integers and also \( q(x) \) is monic.

Hence \( p_0 \alpha \) is an algebraic integer.

**Definition:** Norm of an \( \alpha \) element \( \in \mathbb{D}(D) \) of degree \( n \). Then the product of \( \alpha, \overline{\alpha}, \alpha'' \ldots, \alpha^n \) all are field conjugates of \( \alpha \) is called the norm of \( \alpha \) and it is denoted by \( N_\alpha \).

\[ N_\alpha = \alpha \overline{\alpha} \alpha'' \ldots \alpha^n \]

**Theorem:** The norm of an algebraic integer is a rational integer.

**Proof:** Let \( \alpha \) be an algebraic integer and let \( P(x) = x^n + s_1 x^{n-1} + \ldots + s_m \) be the defining polynomial of \( \alpha \); and

\[ f(x) = (x - \alpha) (x - \overline{\alpha}) (x - \alpha') \ldots (x - \alpha^n) \]

where \( \alpha', \alpha'', \ldots, \alpha^n \) are the conjugate of \( \alpha \).

\[ f(x) = \left[ P(x) \right]^{n/m} \]
\[(a - a') (a - a'') \cdots (a - a'^m) = [P(a)]^{m/m}\]
\[= (a - a') (a - a'') \cdots (a - a'^m)\]
\[= [x^m + s_1 x^{m-1} + \cdots + s_m]^{m/m}\]

Comparing the constant terms of both polynomials, we have:
\[a^m - a'^m - \cdots - a'^m = (s_m)^{m/m}.\]
\[N_a = (s_m)^{m/m}.

Norm of \(a\) is a power of \(s_m\) where \(s_m\) is an integer. Hence \(N_a\) is a rational integer.

**Theorem:** If \(a\) and \(b\) are elements of \(R(a)\), then

\[N_{ab} = N_a N_b.\]

**Proof:** Let \(p(x) = x^n + s_1 x^{n-1} + \cdots + s_m\) be the defining polynomial of \(a\).

and let

\[p(x) = x^n + s_1 x^{n-1} + \cdots + s_m\]
\[ g(m) = m - 1 \]

if \( m \) is prime.

if \( m \) is not prime.

\[ m = B_1 \cdot B_2 \cdot \ldots \cdot B_r \]

\[ g(m) = \left( \sum_{i=1}^{r} B_i \right) - 1 \]

\[ = 16 \left( 1 - \frac{1}{2} \right) \]
ASSIGNMENT  

$E(Y) = g(Y_0, X_1) - 61(Y_0 - y_0)$

From eqn (3)

$q_1(x_0 - x_1) = b_1(y_0 - y_1)$

$\frac{b_1}{a_1(x_0 - x_1)}$

where $(a_1, b_1) = \ldots$

Then

$x_i = x_0 - x_1 = \text{bit} \implies x_1 = x_0 - \text{bit}$

$x_i = x_0 - b_i \implies x_i = x_0 - \frac{b_i}{a_i}$ from eqn (3)

$q_1(x_0 - y_0 + \text{bit}) = b_1(y_0 - y_1)$

$q_1 \text{bit} = b_1(y_0 - y_1)$

$q_1 \text{bit} = \ldots$

$q_1 \text{bit} = \ldots$

$q_1 \text{bit} = \ldots$

$y_1 = y_0 + \text{bit}$

$y_i = y_0 + \frac{a_i}{b_i}$

$E(X) = \sum \left( x_i - \frac{b_i}{a_i} \right) (x_0 + \frac{a_i}{b_i})$
Theorem:

Let \( f \) be a bounded function and \( E \) be a measurable set of finite measure. Then for simple functions \( \psi \) and \( \eta \) show that

\[
\int_E \psi(x) \text{d}x = \sup_{\eta \leq \psi} \int_E \eta(x) \text{d}x \quad \text{if} \quad \eta \leq f
\]

Proof: Suppose that \( f \) is bounded by \( M \) and \( f \) is measurable. Then see

\[
E_n = \left\{ \frac{\int_E f(x) \text{d}x}{n} \geq \frac{m(M-1)}{n} \right\} = \bigcup_{k=1}^{n}
\]

are measurable disjoint and have union \( E \) i.e.

\[
m(E) \leq mE \Rightarrow \exists \frac{m(mE)}{n} = mE.
\]

The simple function is defined as:

\[
\psi_n(x) = M \sum_{k=1}^{n} \chi_{E_k}(x)
\]

and

\[
\eta_n(x) = M \sum_{k=1}^{n} (k-1) \chi_{E_k}(x)
\]

satisfy

\[
\psi_n(x) \geq f(x) \geq \eta_n(x)
\]

\[
\eta_n(x) \leq f(x) \leq \psi_n(x)
\]

Thus

\[
m \int_{E} \psi_n(x) \text{d}x \leq \int_{E} \psi(x) \text{d}x \leq M \sum_{k=1}^{n} mE_k
\]

\[
\sup_{E} \int_{E} \eta_n(x) \text{d}x \geq \int_{E} \eta(x) \text{d}x \leq M \sum_{k=1}^{n} (k-1) mE_k
\]
we have

\[ 0 \leq \inf_{E} \int \Psi_{n}(x) \, dx - \sup_{E} \Psi_{n}(x) \leq M(\text{max} \, \Psi_{n}) \]

Since \( n \) is arbitrary,

\[ \inf_{E} \int \Psi_{n}(x) \, dx - \sup_{E} \Psi_{n}(x) \downarrow 0 \]

\[ \Rightarrow \inf_{E} \int \Psi_{n}(x) \, dx = \sup_{E} \Psi_{n}(x) \]

\[ \Psi \geq \frac{1}{2} \Psi \Phi \]

Conversely, suppose that

\[ \inf_{E} \int \Psi_{n}(x) \, dx = \sup_{E} \Psi_{n}(x) \] for all \( n \).

Then given \( \varepsilon > 0 \), there is a simple gen \( \eta_{n} \) of \( x \) and \( \Psi_{n} \) such that \( x \leq \eta_{n}(x) \leq \Psi_{n}(x) \).

\[ \int \Psi_{n}(x) \, dx - \int \eta_{n}(x) \, dx < \varepsilon \]

Then the function

\[ \Psi^{*} = \sup \Psi_{n} \] and \( \Phi^{*} = \sup \Phi_{n} \)

are measurable by theorem and.

\[ \Psi^{*} \leq \Phi^{*} \]

now the set

\[ \Delta = \left\{ x : \Phi^{*}(x) < \Psi^{*}(x) \right\} \]

is the union of the sets

\[ A_{\varepsilon} = \left\{ x : \Phi^{*}(x) < \Psi^{*}(x) - \frac{1}{\varepsilon} \right\} \]
But each \( A_\nu \) is contained in the set

\[
A_\nu = \{ x; f(x) < y_\nu(x) - \frac{1}{\nu} \}
\]

and the latter set has measure less than \( \nu m \). Since \( \nu \) is arbitrary; \( m(A_\nu) = 0 \) and \( m_A = 0 \). Thus \( p^* \) and \( \bar{p}^* \) except on a of measure zero. Thus \( f \) is measurable.

**Note:**

\[
\inf_{\nu} \left( \frac{f}{\nu} \right) = \bar{f} \quad \text{and} \quad \sup_{\nu} \left( \frac{f}{\nu} \right) = \underline{f}.
\]

**Bounded Egoroff Theorem:**

Let \( \{ f_\nu \} \) be a sequence of measurable functions defined on a set \( E \) of finite measure bounded by \( M \) i.e. \( |f_\nu(x)| \leq M \)

and \( \lim \limits_{\nu \to \infty} f_\nu(x) = f(x) \) for each \( x \in E \).

Then

\[
\left( f(x) = \lim \limits_{\nu \to \infty} f_\nu(x) \right) \quad \text{for each} \quad x \in E.
\]

**Proof:** Suppose that \( f(x) = \lim \limits_{\nu \to \infty} f_\nu(x) \) for each

for given \( \varepsilon > 0 \), there is natural \( no \) and a subset \( A \subset E \) s.t. for all \( n > N \).

Then

\[
|f_\nu(x) - f(x)| < \frac{\varepsilon}{2M} \quad \text{for} \quad x \in E.
\]

we have.
\[ \left\lvert \int \left( f_n(x) - f(x) \right) \, dx \right\rvert = \left\lvert \int f_n - f \bigg|_E \right\rvert \leq \int \left\lvert f_n - f \right\rvert \, dx \]

Now

\[ \int \left\lvert f_n - f \right\rvert < \frac{\varepsilon}{2mE} \leq \frac{\varepsilon}{2} \]

Next

\[ \left\lvert f_n(x) - f(x) \right\rvert \leq \left\lvert f_n(x) \right\rvert + \left\lvert f(x) \right\rvert \leq 2M. \]

\[ \int \left\lvert f_n - f \right\rvert < \frac{\varepsilon}{2} \]

Using (i) and (ii) in eqn (i)

\[ \left\lvert \int f_n - f \right\rvert < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \]

\[ \int f_n - f \bigg|_E \]
Case III. If \( c < 0 \implies -c > 0 \) then \((-c)^+ \) and \((-c)^- \) are non-negative functions. 

\[
\begin{align*}
E &= (-c)^+ + (-c)^- \\
E &= \int_{E} (-c)^+ + (-c)^- \\
E &= -c \left[ \int_{E} f^- + c \int_{E} f^+ \right] \\
&\quad - c \left[ \int_{E} f^+ - \int_{E} f^- \right] \\
\end{align*}
\]

(iii) \( f \leq g \) (a.e.)

\( 0 \leq f - g \) (a.e).

Since integral over \( g \) non-negative and \( f \) non-negative,

\[
0 = \int_{E} g - f = \int_{E} g - \int_{E} f \\
\implies \int_{E} f \leq \int_{E} g.
\]

(iv) \( \int_{A \cup B} f = \int_{A \cup B} f \) (a.e.)

\[
\int_{A \cup B} f = \int_{A \cup B} f \triangleleft \int_{A \cup B} f (A + B) \\
= \int_{A \cup B} f A + \int_{B \setminus A} f B \\
\]

Section 2. The Congruences,

1) By substituting the integers in the e.r.s.

2) \( ax \equiv b \pmod{m} \)

The diophantine prime \( ax + my = b \)

3) A linear congruence \( ax \equiv b \pmod{m} \) whose \( (a, m) = 1 \) can sometimes be solved easily by adding or subtracting suitable multiple of \( m \) such that coefficient of \( x \) divides the other side.

For e.g.,

\[ 3x \equiv 4 \pmod{5} \]
\[ x \equiv 3, 4 \pmod{5} \]
\[ 3x = 9 \pmod{5} \]
\[ x = 3, 8 \pmod{5} \]

\( x = 3 \pmod{5} \) is the solution of the given congruence.

4) Sometimes it is possible to find the solution of the congruence \( ax \equiv b \pmod{m} \), \( (a, m) = 1 \) with the Euler's Theorem.

By putting \( a \equiv b \pmod{m} \)

For e.g.,

\[ 4x \equiv 7 \pmod{9} \]
\[ 4(9) = 6 \]
\[ x \equiv 7, 4 \pmod{9} \]
\[ x \equiv 4 \pmod{9} \]
Show that Möbius function is multiplicative.

\[ \mu(m \cdot n) = \mu(m) \cdot \mu(n) \]

Let \( m = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots \cdot p_k^{a_k} \),

\[ n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots \cdot p_l^{b_l} \]

\[ mn = p_1^{a_1 + b_1} \cdot p_2^{a_2 + b_2} \cdot p_3^{a_3 + b_3} \cdots \cdot p_k^{a_k} \cdot p_l^{b_l} \]

\[ \mu(mn) = \mu(p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots \cdot p_k^{a_k} \cdot p_l^{b_l}) \]

\[ = \mu(m) \cdot \mu(n) \]

\[ \mu(m) = 0 \quad \text{if any } a_i > 0 \]

\[ \mu(n) = 0 \quad \text{if } a_i > 0 \]

\[ \mu(mn) = \begin{cases} \mu(m) \cdot \mu(n) & \text{if } a_i > 0 \text{ for any } i \end{cases} \]

\[ \mu(8) = 2^3 \]

\[ \mu(12) = 2^2 \times 3 \]

\[ \mu(96) = 2^5 \times 3 \]

Show that

\[ d(mn) = d(m) \cdot d(n) \]

\[ \sigma(mn) = \sigma(m) \cdot \sigma(n) \]
Theorem

Proof of Theorem

If \( p \) is an odd prime, then the integer \( \alpha \) is a quadratic residue
\[ \alpha \equiv \alpha \left( \text{mod} \ p \right) \]

Proof: Suppose that \( \alpha \) is a quadratic residue of \( p \). Then,
\[ \alpha^2 \equiv 1 \left( \text{mod} \ p \right) \]

Since \( p \) is odd prime, therefore,
\[ \alpha^2 \equiv \alpha \left( \text{mod} \ p \right) \]

Let \( \varphi(p) = p-1 \), so
\[ (\alpha^2)^{\varphi(p)} \equiv \alpha^{2\varphi(p)} \left( \text{mod} \ p \right) \]

Since \( (\alpha, p) = 1 \), therefore by Fermat's Theorem
\[ \alpha^{p-1} \equiv 1 \left( \text{mod} \ p \right) \]

So
\[ \alpha^{\varphi(p)} \equiv 1 \left( \text{mod} \ p \right) \]

Conversely, suppose that
\[ a^2 \equiv 1 \pmod{p} \]

and consider

\[ x^2 = a \pmod{p}, \]

let \[ x \equiv a^{\frac{p-1}{2}} \pmod{p} \]

\[ (a^{\frac{p-1}{2}})^2 = a \pmod{p}. \]

Since \[ a^{p-1} \equiv 1 \pmod{p} \],

\[ a \equiv 1 \pmod{p}. \]

\[ (a^{\frac{p-1}{2}})^2 = 1 \pmod{p}. \]

\[ x^2 \equiv a \equiv 1 \pmod{p}. \]

\[ x \equiv a \equiv 1 \pmod{p}. \]

The solution of

\[ x^2 \equiv a \pmod{p}, \]

Hence \[ a \] is the residue of \[ x \] in \[ p \].
Theorem 19

\[ n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \]

where \( p_i \)'s are distinct primes. Then show that

\[ \begin{align*}
\text{i) } \quad d(n) &= \prod_{i=1}^{k} (a_i + 1), \\
\text{ii) } \quad \sigma(n) &= \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.
\end{align*} \]

Proof: Since \( p_i \)'s is prime, then the only divisor of \( n \) are \( p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \).

\[ \Rightarrow d(P_i^{a_i}) = a_i + 1. \]

Then

\[ d(P_i^{a_1}, P_j^{a_2}, \ldots, P_k^{a_k}) = d(P_i^{a_1}) d(P_j^{a_2}) \cdots d(P_k^{a_k}). \]

\[ \begin{align*}
2^n - 1 &= \prod_{i=1}^{k} (a_i + 1), \\
2^n + 1 &= (a_1 + 1)(a_2 + 2) \cdots (a_k + 1).
\end{align*} \]

and

\[ \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \]

\[ O(P_i^{a_i}) = 1 + P_i + P_i^2 + \cdots + P_i^{a_i} \]

is Geometric Series: \( \leq \frac{a_i^{a_i+1}}{a_i - 1} \)

\[ O(P_i^{a_i}) = \frac{P_i^{a_i+1} - 1}{P_i - 1}. \]
Perfect number. A number is said to be perfect if its sum of the divisors can be expressed as

\[ \sigma(n) = 2n. \]

Note: All perfect numbers are even.

Theorem: An even integer is perfect if and only if it is of the form

\[ 2^{p-1} (2^p - 1) \]

where \( 2^p - 1 \) is prime.

\[ d(n) \] is odd \iff \( n \) is a square.

If \( d(n) \) is odd then \( n \) is square.

Every integer \( n \geq 1 \) has prime divisors.

Every composite number \( n \) has prime divisors \( \leq \sqrt{n} \).

If \( n \) and \( k \) are \( \geq 2 \) then \( \left[ \frac{nk}{k} \right] \geq \left[ \frac{n}{k} \right] + \left[ \frac{k}{k} \right] \).

If \( n \) is positive integer and \( ak \) then number of multiple of \( n \) is \( \leq \left[ \frac{x}{n} \right] \).

Proof: The multiple of \( n \) \( \leq x \) are the following integers:

\[ m_n, 2n, 3n, \ldots, m_n \]

where \( m_n \) is the largest multiple of \( \frac{n}{n} \).

\[ m_n \leq x \leq (m_n+1) \frac{n}{n} \]

\[ m_n \leq \frac{x}{n} \leq m_n+1 \]

\[ 0 \leq \frac{x}{n} - m_n < 1. \]

\[ \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor - m_n + 1 = 0 \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor = m_n. \]
Since

\[ x_1 = [x_1] + 0, \quad x_2 = [x_2] + 0, \]

\[ x_1 + x_2 = [x_1] + [x_2] + 0 + 0. \]

\[ [x_1 + x_2] = [x_1] + [x_2], \]

if \( 0 \leq 0 + 0 < 1. \)

Hence

\[ [x_1 + x_2] > [x_1] + [x_2]. \]

Theorem: If \( n \) is an integer \( > 0 \) then.

The highest power of a prime \( p \) which divides \( n! \) is

\[ \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \]

\[ - \] Number of integers which are \( \leq n \) and divisible by \( p \) is

\[ \left\lfloor \frac{n}{p} \right\rfloor \]

and these integers are

\[ p, 2p, 3p, \ldots, \left\lfloor \frac{n}{p} \right\rfloor \cdot p. \]

\[ - \] Find the highest power of 7 dividing

The integer 1001

\[ \left\lfloor \frac{1001}{7} \right\rfloor + \left\lfloor \frac{1001}{7^2} \right\rfloor + \left\lfloor \frac{1001}{7^3} \right\rfloor + \cdots \]

\[ = 14 + 2 + 0 + 0 \]

\[ = 16. \]
Lagrange's Theorem is not true if \( p \) is not prime.

Give the congruence

\[ 4n^2 + 4n - 1 \equiv 0 \pmod{7} \]

The given congruence can be written as,

\[ 4n^2 + 4n + 1 \equiv 2 \pmod{7} \]

adding \( 4 \)

\[ (2n+1)^2 \equiv 3^2 \pmod{7} \]

\[ 2n+1 \equiv \pm 3 \pmod{7} \]

\[ 2n = 2 \pmod{7} \]

and

\[ 2n = -4 \pmod{7} \]

\[ n = 1, 2 \pmod{7} \]

\[ n = 1, 5 \pmod{7} \] are the possible solutions of the given congruence.

ii) \[ x^3 - 4x^2 + 5x - 6 \equiv 0 \pmod{27} \]

First, we solve

\[ x^3 - 4x^2 + 5x - 6 \equiv 0 \pmod{3} \]

Trying \( x = 0, 1, 2 \) we find \( x = 0 \pmod{3} \) is the only solution.

Let \( x = 3t + r \).
Show that 33 is quadratic non-
residue of 89.

So, we are to show that

\[ \left( \frac{33}{89} \right) = -1. \]

Since \[ \left( \frac{33}{89} \right) = \left( \frac{3}{89} \right) \left( \frac{11}{89} \right) \]

First we check:

\[ \left( \frac{11}{89} \right) \text{ applying the reciprocity law} \]

\[ \left( \frac{11}{89} \right) \left( \frac{89}{11} \right) = \left( \frac{11-1}{89-1} \right) = (-1) \cdot \frac{11-1}{89-1} \]

\[ = (-1)^{89-1} \left( \frac{11}{89} \right) \]

\[ = 1 \]

\[ \Rightarrow \left( \frac{11}{89} \right) \left( \frac{89}{11} \right) \text{ both have same quadratic character.} \]

Since

\[ 89 \equiv 1 \mod 11 \]

Since

\[ \alpha^2 \equiv 1 \mod 11 \]

has 827

\[ \alpha \equiv 1 \mod 11 \]

So

\[ \left( \frac{1}{11} \right) = 1 \]

These

\[ \left( \frac{89}{11} \right) = 1 \]

Now we check \( \left( \frac{3}{89} \right) \).
\[
\left( \frac{3}{89} \right) \left( \frac{89}{3} \right) = (-1)^{\frac{89-1}{2}} \cdot \left( \frac{2}{3} \right) \cdot \left( \frac{3}{89} \right)
\]

Both have same quadratic character.

Since
\[
89 = 2 \cdot (29)
\]
\[
\frac{89}{3} = \frac{2}{3}
\]

Since 29 is odd prime
\[
\left( \frac{2}{3} \right) = (-1)^{\frac{2-1}{2}} = (-1)^{\frac{1}{2}} = -1
\]

\[
\left( \frac{89}{3} \right) = -1
\]

Hence
\[
\left( \frac{89}{3} \right) = \left( \frac{2}{3} \right) \cdot \left( \frac{89}{3} \right) = (-1) \cdot (-1) = 1
\]

Hence 89 is a non-quadratic residue.

Show that
\[
\frac{67}{89}
\]

Since
\[
67 = -22 \pmod{89}
\]

\[
89 \left( \frac{-22}{89} \right) = \left( \frac{-1}{89} \right) \left( \frac{2}{89} \right) \left( \frac{11}{89} \right)
\]

\[
= (-1)^{\frac{89-1}{2}} \cdot (-1)^{\frac{89-2}{2}} \cdot \left( \frac{89}{8} \right)
\]
\[
\left( \frac{11}{89} \right) \left( \frac{89}{11} \right) = (-1)^{\frac{11-1}{2}} \frac{89-1}{2} = 1
\]

In \( \frac{11}{89} \), \( 89/11 \) have same character

\[
\left( \frac{89}{11} \right) = \left( \frac{1}{11} \right) = 1
\]

\[
\left( \frac{11}{89} \right) = 1
\]

Hence \( \left( \frac{67}{89} \right) = \left( \frac{-22}{89} \right) = 1 \)

Hence 67 is quadratic residue \( \mod 89 \)

\[
1) \quad \frac{182}{271}
\]

Since

\[
182 = -89 \quad (\mod 271)
\]

\[
-\frac{89}{271} = -\frac{1}{271} \cdot \frac{89}{271}
\]

\[
= \left( \frac{-1}{271} \right) \cdot \frac{89}{271}
\]

\[
= \left( \frac{-1}{271} \right)^{\frac{271-1}{2}} \cdot \frac{89}{271}
\]

\[
= (-1)^{\frac{271-1}{2}} \cdot \frac{89}{271}
\]

\[
= \left( \frac{89}{271} \right)
\]

\[
\left( \frac{89}{271} \right) \left( \frac{271}{89} \right) = (-1)^{\frac{14 \cdot 185}{2}} = 1
\]

Applying reciprocity law
Hence

\[
\begin{align*}
\left( \frac{89}{271} \right) & \neq \left( \frac{271}{89} \right) \quad \text{both have character-}
\end{align*}
\]

\[
\begin{align*}
0, \quad \left( \frac{271}{89} \right) & = \frac{4}{89}, \\
4 & \equiv -85 \quad (\text{mod } 89) \\
\frac{-85}{89} & = (-1) \left( \frac{5}{89} \right) \left( \frac{17}{89} \right), \\
& = (-1)^2 = 1
\end{align*}
\]

Both \( \left( \frac{5}{89} \right) \left( \frac{17}{89} \right) \) have the quadratic character.

\[
\begin{align*}
\left( \frac{89}{271} \right) & = \frac{135}{5840} \\
& = (-1) \cdot (-1)
\end{align*}
\]

Hence 182 is quadratic non-

\[
\begin{align*}
\text{Resolve of 271:} \\
\text{mod } 3 & \quad 1188, \\
\text{mod } 7 & \quad 3, 63, 21, 17
\end{align*}
\]

\[
\begin{align*}
\left( \frac{283}{997} \right) & \equiv -188 \quad (\text{mod } 997). \\
\left( \frac{283}{997} \right) & = \left( - \frac{188}{997} \right) \left( \frac{189}{997} \right) \left( \frac{7}{997} \right)
\end{align*}
\]

\[
= 1.
\]
Prove that:

1) \( x = \lfloor x \rfloor + \delta \quad 0 \leq \delta < 1 \)
2) \( \lfloor x + n \rfloor = \lfloor x \rfloor + n \quad x \in \mathbb{R}, \ n \in \mathbb{Z} \)

If \( xy \in \mathbb{R}, y \geq 0 \) and:
\[ x = y + \delta \quad \text{where} \quad 0 \leq \delta < 1 \]
Then:
\[ \lfloor x \rfloor = y \]

ii) \[ \lfloor x \rfloor = \lfloor \frac{x}{n} \rfloor \]

**Proof:**

i) \( x = \lfloor x \rfloor + \delta \quad 0 \leq \delta < 1 \)
   - True by definition.

ii) Prove that \( \lfloor x + n \rfloor = \lfloor x \rfloor + n \)

Since \( \delta = \lfloor x \rfloor + \theta \quad 0 \leq \theta < 1 \)
\[ \lfloor x \rfloor = \lfloor x - \delta \rfloor \]
add n to both sides:
\[ \lfloor x \rfloor + n = \lfloor x + n \rfloor + \delta + 0 \]
\[ \lfloor x \rfloor + n = \lfloor x + n \rfloor + \Theta \quad 0 \leq \Theta < 1 \]

Thus:
\[ \lfloor x \rfloor, n, \text{ and } \lfloor x + n \rfloor \text{ are integers so } \]
\( \delta + \Theta \) must be integer but
\[ 0 \leq \Theta - \delta < 1 \]
\[ \delta - \Theta = 0 \quad \checkmark \]

Since:
\[ \lfloor x \rfloor + n = \lfloor x + n \rfloor \]
\[ y = x \cdot y \\]

Then
\[ \left[ \frac{x}{y} \right] = 1. \]

Since
\[ x = y \cdot \theta, \]

Dividing on both sides by \( y \),
\[ \frac{x}{y} = \theta + \frac{\theta}{y}. \]

taking \( \approx \)kered \facion,
\[ \left[ \frac{x}{y} \right] = \left[ \theta + \frac{\theta}{y} \right] \]
\[ = \left[ \theta + \left[ \frac{\theta}{y} \right] \right] : \theta \in \mathbb{Z}. \]

Since \( 0 \leq \theta < y \) therefore

by definition
\[ \left[ \frac{\theta}{y} \right] = 0 : 0 < \frac{\theta}{y} < 1. \]

Hence
\[ \left[ \frac{x}{y} \right] = 1. \]

Hence Prove \( \frac{x}{y} \)
Proof that 
\[
\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor.
\]  

Since \( \lfloor x \rfloor \in \mathbb{Z} \) so \( \lfloor x \rfloor = \hat{x} + q \) and \( 0 \leq q < 1 \) and \( \lfloor \hat{x} \rfloor = \hat{x} \), we have 
\[
\lfloor x \rfloor = \hat{x} + q.
\]

Then 
\[
x = \lfloor x \rfloor + \theta = \hat{x} + q + \theta.
\]

Hence, 
\[
\lfloor x \rfloor = \hat{x} + q + \theta.
\]

Therefore, 
\[
\frac{x}{n} = \frac{\hat{x} + q + \theta}{n}.
\]

Also, 
\[
\frac{\lfloor x \rfloor}{n} = \frac{\hat{x}}{n} + \frac{q}{n} + \frac{\theta}{n}.
\]

Since \( \hat{x} \) is an integer, then 
\[
\left\lfloor \frac{\hat{x}}{n} \right\rfloor = \hat{x}.
\]

Thus, 
\[
\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{\hat{x} + q + \theta}{n} \right\rfloor.
\]
Theorem \[ \left[ \begin{array}{c} x \\ y \\ z \\ \end{array} \right] = \left[ \begin{array}{c} p-1-z \\ x \\ \end{array} \right] \mod p \]

Since \( x, y \in \mathbb{Z} \), there exists \( \nu \) such that \( x = \nu \).

\[ y = qy + \nu \]

\[ \alpha = \sigma \]

\[ \left[ \begin{array}{c} x \\ y \\ z \\ \end{array} \right] = \left[ \begin{array}{c} qz + \nu \\ x \\ \end{array} \right] \mod p \]

\[ \frac{qz + \nu}{qy + \nu} = \sigma \]

\[ \sigma = a \mod p \]

\[ X = \sigma \]

\[ \frac{qz + \nu}{qy + \nu} = a \mod p \]

\[ X = \sigma \]

\[ \frac{qz + \nu}{qy + \nu} = a \mod p \]

\[ \sigma = a \mod p \]

\[ X = a \]
\[ q(mn) = q(m) q(n), \]

12 = 4 \cdot 3 = 2^2 \cdot 3^1

\[ q(m) = \begin{cases} \frac{m}{p_i^{a_i}} & \text{if } m > 1, \\ \end{cases} \]

\[ m = p_1^{a_1} p_2^{a_2} \ldots \]

**be the standard form of \( m \).**

Then

\[ q(m) = \frac{m}{p_i^{a_i}}, \quad \prod_{i=1}^\gamma p_i^{a_i}, \quad \prod_{i=1}^\gamma (p_i^{a_i} - 1) \]

or

\[ q(m) = m \prod_{i=1}^\gamma (1 - \frac{1}{p_i}) = m \prod_{i=1}^\gamma (1 - \frac{1}{p_i}) \]

**Proof:**

Let \( p \) be the standard factorization of \( m \). Then there are exactly \( p^a \) integers not exceeding \( p^a \) which are relatively prime to \( p^a \) so remaining \( p^a - p^a - 1 \) will be relatively prime to \( p \), i.e.

\[ q(p^a) = p^a - p^a - 1 = p^a (1 - \frac{1}{p}) \]
Similarly,

\[ q(p_{i+1}^{a_i}) = p_{i+1}^{a_i} \left(1 - \frac{1}{p_i}\right) \]

\[ q(p_{2}^{a_2}) = p_{2}^{a_2} \left(1 - \frac{1}{p_2}\right) \]

\[ q(p_{r}^{a_r}) = p_{r}^{a_r} \left(1 - \frac{1}{p_r}\right) \]

Since

\[ m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \]

\[ q(m) = q(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \]

\[ = q(p_{i+1}^{a_i}) q(p_{2}^{a_2}) \cdots q(p_{r}^{a_r}) \]

\[ = p_{i+1}^{a_i} \left(1 - \frac{1}{p_i}\right) \cdot p_{2}^{a_2} \left(1 - \frac{1}{p_2}\right) \cdot p_{3}^{a_3} \left(1 - \frac{1}{p_3}\right) \cdots p_{r}^{a_r} \left(1 - \frac{1}{p_r}\right) \]

\[ = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \]

\[ = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \]

\[ = m \prod_{l=1}^{r} \left(1 - \frac{1}{p_l}\right) \]

\[ = \prod_{l=1}^{r} p_l^{a_l} \left(p_l - 1\right) \]
Since

\[ \phi(m) = \phi_1 \cdot \phi_2 \cdots \phi_r \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \]

\[ = \prod_{i=1}^{r} p_i \left(1 - \frac{1}{p_i}\right) \]

\[ = \prod_{i=1}^{r} p_i (p_i - 1) \]

\[ \phi(m) = \prod_{i=1}^{r} p_i (p_i - 1) \]

\[ \phi(500) = ? \]

\[ \phi(500) = 500 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \]

\[ = 500 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) \]

\[ = \frac{500 \times 4}{10} = 200 \]

i.e. exactly 200 positive integers are relatively prime to 500.
\[
\begin{align*}
\varphi(7562) &= \varphi(2 \cdot 8781) \\
&= \varphi(2) \cdot \varphi(8781) \\
&= 1 \cdot 8780 \\
&= 8780 = 2 \cdot 8781 \\
5000 &= 2 \cdot 5^2 \\
\end{align*}
\]}

Hence, \[
\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).
\]

\[
\begin{align*}
\varphi(5000) &= 5000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\
&= 5000 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) \\
&= 2000
\end{align*}
\]
Prove that \( q(m^2) = m \cdot q(m) \).

**Proof:**

Let \( m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r} \) be the standard form of \( m \). Then

\[
m^2 = p_1^{2a_1} \cdot p_2^{2a_2} \cdots p_r^{2a_r}
\]

Also,

\[
q(m) = m \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right).
\]

Now,

\[
q(m^2) = m^2 \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right).
\]

\[
= m \cdot m \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right)
\]

\[
= m \cdot q(m).
\]

Hence,

\[
q(m^2) = m \cdot q(m)
\]

**Generally,**

\[
q(m^n) = m^{n-1} \cdot q(m)
\]

Under decision...
Let $A'$ be a C.R.S and $B$ a subset of $A'$ containing all those members of $A'$ which prime to $m$. Then $B$ is R.R.S. (mod $m$) for e.g. $m = 7$. Then c.r.s.(mod 7)

$A = \{0, 1, 2, 3, 4, 5, 6\}$.

$B = \{1, 2, 3, 4, 5, 6\}$ is R.R.S.(mod 7)

If $m = 8$.

$A = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

C.R.S. Then $\varphi(8) = 4, \ (3) = 3$.

$B = \{1, 3, 5\}$.

$3 \neq 5$ (mod 8).

Def.: $A$ see $A'$ is R.R.S. (mod $m$)

i) $A'$ has $\varphi (m)$ elements.

ii) If $a_i \in A$ then $(a_i, m) = 1$

iii) If $a_i, a_j \in A$ & $i \neq j$ then $a_i \neq a_j$ (mod $m$)

$\forall a_i \in A \ a_i \equiv x_i$ for some $x_i \in A$.
Result: Corollary: If \( m > 2 \) then 
\[ \Phi(m) \text{ is always even.} \]

If \( \{a_1, a_2, a_3, \ldots, a_{\Phi(m)}\} \) is a \( \text{R.R.S (mod m)} \) and 
\[ \Phi(m) = 1 \] then \( A = \{a_1, a_2, \ldots, a_{\Phi(m)}\} \) 
is also a \( \text{R.R.S (mod m)}. \)

Proof: As \( A = \{a_1, a_2, \ldots, a_{\Phi(m)}\} \),

\[ a \text{ is clearly a } \Phi(m) \text{ elements.} \]

\[ a_i \neq a_j \text{ for } i \neq j \]

\[ a_i = a_j \text{ (mod m)} \]

\[ a_i - a_j = 0 \text{ (mod m)} \]

\[ a(a_i - a_j) = 0 \text{ (mod m)} \]

\[ a_i - a_j = 0 \text{ (mod m)} \text{ since } (a, m) = 1 \]

\[ a_i = a_j \text{ (mod m)} \]

which is a contradiction as \( a_i \) and \( a_j \) are elements of \( \text{R.R.S} \) hence our supposition is wrong and

\[ a_i \neq a_j \text{ (mod m)} \text{ for } i \neq j \]

\[ (a_i, m) = 1 \text{ for } i = 1, 2, 3, \ldots, \Phi(m) \]

\[ (a_i, m) = 1 \]

All the three conditions satisfied.

Hence \( A \) is \( \text{R.R.S.} \)
write \( \mathbb{C} \mathbb{R} \mathbb{S} \mathbb{P} \) modulo 17 as multiple of 3.

b) write \( \mathbb{R} \mathbb{S} \mathbb{P} (\mod 17) \) as multiple of 3.

\[ \text{Sol. -} \]

for \( m = 17 \):

\( \mathbb{C} \mathbb{R} \mathbb{S} \mathbb{P} \) \( (\mod 17) \) as follow:

\[ \begin{cases} 0, 1, 2, 3, \ldots, \frac{16}{2} \\ 0, 3, 6, 9, \ldots, 48 \end{cases} \text{ in } \mathbb{C} \mathbb{R} \mathbb{S} \mathbb{P} (\mod 17), \]

as a multiple of 3.

\[ \begin{cases} 1, 2, 3, 4, 5, \ldots, \frac{16}{2} \\ 3, 6, 9, 12, 15, \ldots, 48 \end{cases} \]

is \( \mathbb{R} \mathbb{S} \mathbb{P} \) as multiple of 3.

\[ \text{Note: if } m \text{ in prime then } \]

\( \mathbb{R} \mathbb{S} \mathbb{P} \) is the maximal proper subset of \( \mathbb{C} \mathbb{R} \mathbb{S} \mathbb{P} \).
If \((\text{gcd}(m,n)) = 1\) then \((m-n, m) = 1\).

\[
\frac{w(x)}{x} = \frac{3x-15}{x} = 3 + \frac{0}{x}
\]

\[
3 + \frac{0}{x} = 16
\]

\[
\text{Proof: we first note that if } (m, n) = 1
\]

\[
\text{then } (m-n, m) = 1
\]

\[
\text{for } (m-n, m) = d
\]

\[
= \frac{d}{m-n}, \frac{d}{m}.
\]

\[
= \frac{d}{m-n} = \frac{d}{m}.
\]

\[
= d, \frac{d}{m}.
\]

\[
= d = 1 \Rightarrow (m, n) = 1.
\]

Hence

\[
(m-n, m) = 1.
\]

Let \(a_1, a_2, a_3, \ldots, a_{\text{(m,n)}}\) be the integers less than \(m\) and prime to \(m\). Then for each \((a_i, m) = 1\):
The set R.R.S.

\[
\Rightarrow (m-a_i, m) = 1
\]

\(m-a_i\) is also one of \(a_1, a_2, a_3, \ldots, a_{\text{(m,n)}}\).

Then \(a_i\) and \(m-a_i\) occurs in the form.

\(8\) pairs among \(a_1, a_2, a_3, \ldots, a_{\text{(m,n)}}\). Then

\[
\frac{a_1 + a_2 + a_3 + \cdots + a_{\text{(m,n)}}}{2} = \frac{1}{2} \left( \frac{a_1 + m - a_1 + a_2 + m - a_2 + \cdots + a_{\text{(m,n)}} + m - a_{\text{(m,n)}}}{2} \right)
\]

\[
= \frac{1}{2} \left( \frac{m + m + m + \cdots + m}{2} \right)
\]

Hence

\[
\Rightarrow \frac{1}{2} m \text{ (mod } m) = (m, \text{ mod } m).
\]
Prove that if \( m > 2 \) then \( q(m) \) is always even.

Proof: if \( m \) is even, then

\[
q(m) = (\frac{m}{2})^{2^s} \text{ if } m + 2 \text{. Then } \]
\[
m = 2a \implies q(m) = q(2^s) \cdot q(p_1, p_2, \ldots, p_r)
\]
\[
= 2^{\frac{a}{2}} (1 - \frac{1}{2}) \text{ since } q(2^s) \text{ is even}
\]
\[
= 2^{\frac{a}{2} - 1} \text{ then } q(m) \text{ is even}
\]
\[
q(m) = 2^{\frac{a}{2} - 1} \text{ if } m \text{ is even.}
\]

Since \( 2 \cdot 2^{s-1} \) is the multiple of \( 2 \)

so \( 2^{s-1} \) is even. Then \( q(m) \) is even.

If \( m \) is odd, then we discuss two cases:

1) \( \text{if } m \text{ is prime.} \)

then \( q(m) = m - 1 \)

since \( m \) is odd. Therefore \( m - 1 \) is even.

Hence \( q(m) \) is even.

2) \( \text{if } m \text{ is not prime.} \)

Then \( m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \text{ where } i = 1, 2, 3, \ldots \)

\( \text{and } p_i \equiv 1 \text{ odd, } \)

\[
q(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right).
\]

Then \( (p_i - 1) \) is even

since each \( p_i \) is odd by prime. Therefore each \( (1 - \frac{1}{p_i}) \) is even. Hence \( q(m) \) is even.

Hence \( m \left(1 - \frac{1}{p_i}\right) \) is even. And \( \left(1 - \frac{1}{p_i}\right) \) is even.

\[
= q(m) \text{ is even.} \]
If $d | n$ then $q(d) | q(n)$.

Let $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$ be the standard form of $n$. Now $d | n$.

Hence the prime factorization of $d$ is $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$. The primes $p_i : i \in \{1, 2, 3, \ldots, r\}$ are among the primes $p_1, p_2, p_3, \ldots, p_r$ and $dij \leq a_i$.

Then $q(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

Also $q(d) = d \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

Now all the factors $\left(1 - \frac{1}{p_i}\right)$ are involved in the product $\frac{q(d)}{q(n)}$.

$\Rightarrow \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

Also $d | n \Rightarrow d \left(1 - \frac{1}{p_i}\right) n \left(1 - \frac{1}{p_i}\right)$ where $\text{se}[m, n] = 1$

$\Rightarrow q(d) | q(n)$ which is the required result.
If \( (a, m) = 1 \), then \( a \equiv 1 \pmod{m} \).

**Proof:**

Let \( A = \{a_1, a_2, a_3, \ldots\} \) be a \( R \cdot R \cdot S \pmod{m} \) and let \( B = \{a_1, a_2, a_3, \ldots\} \) be another \( R \cdot R \cdot S \pmod{m} \). Let \( \{a_i, a_2, a_3, \ldots\} \) be a set of elements of \( B \) but may not in the same order. Then

\[
\text{Let } (5, 6) = 1.
\]

Since each \( (a_i, m) = 1 \) where \( i = 1, 2, 3, \ldots \).

So

\[
(a_1 \cdot a_2 \cdot a_3 \cdots a_n) \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_n \pmod{m}.
\]

Then

\[
25 \equiv 1 \pmod{6}
\]

Since each \( (a_i, m) = 1 \) where \( i = 1, 2, 3, \ldots \).

So

\[
(a_1 \cdot a_2 \cdot a_3 \cdots a_n)^{\frac{m}{n}} = 1; \text{ where } (m, n) = 1 \text{ then } \]

\[
a \equiv b \pmod{m}.
\]

So (i) becomes

\[
1 \equiv a \pmod{m} \text{ or } 0 \equiv a \pmod{m}.
\]

\[
\text{ if } 7 \equiv 8 \pmod{7}
\]

\[
2^7 \equiv 1 \pmod{7}
\]

\[
\frac{7}{1} - 8 \equiv \frac{7}{1} - 8
\]

\[
8 \equiv \frac{7}{1} \pmod{7}
\]

\[
\frac{7}{1} \equiv \frac{7}{1} \pmod{7}
\]
If \( m_1, m_2, m_3, \ldots, m_k \) are positive integers greater than one relatively prime in pairs then system of simultaneous linear congruences

\[
\begin{align*}
\chi &\equiv a_1 \pmod{m_1} \\
\chi &\equiv a_2 \pmod{m_2} \\
& \vdots \\
\chi &\equiv a_k \pmod{m_k}
\end{align*}
\]

has a unique solution \( \pmod{m} \)

where \( m = m_1 \cdot m_2 \cdot m_3 \cdots m_k \).

Proof: let \( M_i = m_1 \cdot m_2 \cdot m_3 \cdots m_{i-1} \cdot m_{i+1} \cdot \cdots m_k \) and \( M_i \cdot m_i \). 

So \( m_i \) is not a factor of \( M_i \).

Since \( m_i \)'s are prime in pair so

\( (M_i, m_i) = 1 \)

Then the linear congruence

\[
M_i \chi \equiv 1 \pmod{m_i}
\]

where \( M_i \neq 0 \pmod{m_i} \); \( m_i \) is not a factor exactly one solution \( \chi \). 

Now consider the integer

\[
\chi = M_1 a_1 + M_2 a_2 + \cdots + M_k a_k.
\]
\[ a \equiv b \pmod{m_i} \]
\[ \Rightarrow a^n \equiv b^n \pmod{m_i} \]
\[ \Rightarrow 8 \equiv 0 \pmod{m_i} \]

\[ y \equiv \sum_{j=1}^{\infty} a_j y_j c_j \]

\[ y \equiv \prod_{i=1}^{k} c_i \pmod{m_i} \]
and
\[ \prod_{i=1}^{k} m_i = m \]

Since
\[ \prod_{i=1}^{k} m_i = m \]
\[ \Rightarrow \prod_{i=1}^{k} m_i y_i c_i \equiv c_i \pmod{m_i} \]

From (4) & (8) by transitive

\[ \Rightarrow y \equiv c_i \pmod{m_i} \]

It means 'y' satisfies all the congruences

\[ x \equiv c_i \pmod{m_i} \]

for 'm_i', i = 1, 2, 3, ... k are relatively prime in pairs. So we have

\[ y \equiv c_i \pmod{m_i} \]

where
\[ m = m_1 m_2 m_3 \cdots m_k \]

For uniqueness, let

\[ z \equiv c_i \pmod{m_i} \]

Then
\[ z \equiv c_i \equiv y \pmod{m} \]
\( x \equiv 2 \pmod{5} \) (mod 7)
\( x \equiv 3 \pmod{5} \)
\( x \equiv 1 \pmod{4} \)

Since \( m_i \)'s are relatively prime in pairs,

\[ \Rightarrow x \equiv y \equiv c_i \pmod{m} \]

So

\[ \Rightarrow x \equiv y \equiv c_i \pmod{m} \] is the unique solution.

Chinese Remainder Theorem

Give the system of congruences:

\[ x \equiv 1 \pmod{4} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 2 \pmod{7} \]

Solve: \[ M_1 = \frac{m_2 \cdot m_3}{m_1} \]

\[ M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35 \]
\[ M_2 = m_1 \cdot m_3 = 4 \cdot 7 = 28 \]
\[ M_3 = m_1 \cdot m_2 = 4 \cdot 5 = 20 \]

\[ M_1 y_1 \equiv 1 \pmod{m_1}, \quad M_2 y_2 \equiv 1 \pmod{m_2} \]
\[ M_3 y_3 \equiv 1 \pmod{m_3} \]

So we have

\[ 35y_1 \equiv 1 \pmod{4} \]
\[ 4 \equiv a-b \pmod{m} \]
\[ \Rightarrow 35y_1 - 4u_1 \equiv 1 \]
\[ \Rightarrow (4 \cdot 8 + 3)y_1 - 4u_1 \equiv 1 \]
\[ \Rightarrow (8y_1 - u_1) + 3y_1 = 1 \]
\[ \Rightarrow 4u_2 + 3y_1 = 1 \]
\[ 4u_2 + 3y_1 = 1 \quad \text{where} \quad u_2 = 8y_1 - u_1 \]

\[ \Rightarrow \quad u_2 = 1 \quad \text{and} \quad y_1 = 1 \]

\[ 28y_2 = 1 \quad \text{(mod 5)} \]

\[ 28y_2 - 5v_1 = 1 \]

\[ (5.5 + 3)y_2 - 5v_1 = 1 \]

\[ 5(5y_2 - v_1) + 3y_2 = 1 \]

\[ 5v_2 + 3y_2 = 1 \quad \text{where} \quad v_2 = 5y_2 - v_1 \]

\[ \Rightarrow \quad v_2 = -1 \quad \text{and} \quad y_2 = 2 \]

\[ y_2 = 2 \quad \text{(mod 5)} \]

\[ 20y_3 = 1 \quad \text{(mod 7)} \]

\[ 20y_3 - 7s_1 = 1 \quad \text{for some} \quad s_1 \in \mathbb{Z} \]

\[ (7.2 + 6)d_3 - 7s_1 = 1 \]
\[ 7(2y_3 - s_1) + 6y_3 = 1 \]

\[ \Rightarrow 7s_2 + 6y_3 = 1 \text{ where} \]

\[ s_2 = 2y_3 - s_1 \]

\[ s_2 = 1, y_3 = -1 \]

\[ 4, -1 \equiv 6 \pmod{7} \quad y_3 = 6 \]

\[ y_3 = 6 \pmod{7} \]

Now,

\[ Y = M_{11}C_1 + M_{22}C_2 + M_3 y_3 C_3. \]

\[ Y = (35)(3)(1) + 28(2)(3) + 20(6)(2) \]

\[ Y = 513. \]

\[ M_{11} \times 7 \]

\[ Y = 93 \pmod{140} \]

is a solution of the system:

\[ 140 | 513 - 93 \]

\[ a - 9 \sqrt{2} - b \]
Solve the system:

\[ x \equiv 2 \pmod{5} \]
\[ x \equiv 3 \pmod{7} \]
\[ x \equiv 5 \pmod{11} \]

Solution:

\[ \begin{align*}
M_1 &= \frac{m_1 m_2 m_3}{m_1} \\
M_2 &= m_2 m_3 = (7)(11) = 77 \\
M_3 &= m_1 m_2 = (5)(7) = 35 \\
M_1 y_1 &\equiv 1 \pmod{m_1} \\
27 y_1 &\equiv 1 \pmod{m_1} \\
\Rightarrow 27 y_1 - 5 y_1 &= 1 \\
(5(10y_1 + 2y_1) - 5y_1 &= 1 \\
\Rightarrow 5 (15y_1 - 5y_1) + 2y_1 &= 1 \\
5u_2 + 2y_1 &= 1 \quad \text{where } 15y_1 - 5y_1 = u_2 \\
5(2 + 3)u_2 + 2y_1 &= 1 \\
2(u_2 + y_1) + 3u_2 &= 1 \quad \text{where } u_2 + y_1 = u_3 \\
2u_3 + 3u_2 &= 1 \\
u_3 &= 3, \quad u_2 = -2, \quad y_1 = 5
\end{align*} \]
\[ y_1 = 5 \pmod{7} \]
\[ M_2 y_2 = 1 \pmod{m_2} \]
\[ 5y_2 = 1 \pmod{7} \]
\[ 5y_2 - 7u_1 = 1 \]
\[ (7(8y_2 - y_2)) - 7u_1 = 1 \]
\[ 7(y_2 - u_1) - y_2 = 1 \]
\[ 7u_2 - y_2 = 1 \]
\[ u_2 = 8y_2 - u_1 \]
\[ u_2 = 1 \]
\[ y_2 = 6 \]
\[ y_2 = 7 \]
\[ \sqrt{y_2 = 7 \pmod{7}} \]
\[ 48 \equiv 3 \pmod{5} \]
\[ M_3 y_3 = 1 \pmod{m_3} \]
\[ 3y_3 = 1 \pmod{11} \]
\[ 3y_3 - 11u_1 = 1 \]
\[ (11(3y_3) + 2y_3) - 11u_1 = 1 \]
\[ 11(3y_3 - u_1) + 2y_3 = 1 \]
\[ u_2 + 2y_3 = 1 \]
\[ u_2 = 1 \]
\[ y_3 = -5 \]
\[ -5 \equiv -5 \pmod{11} \]
\[ y_3 = 11 \pmod{11} \]
\[ y_3 = 6 \pmod{11} \]
Now

\[ Y = M_1 J_1 C_1 + M_2 J_2 C_2 + M_3 J_3 C_3. \]

\[ Y = 77(5)(2) + 55(7)(3) + 77(11)(5) \]

\[ Y = 770 + 1155 + 385 \]

\[ Y = 2310 \]

\[ Y \equiv 14 \pmod{82}. \]
**Theorem**

Every composite number \(n\) has a prime divisor \(\leq \sqrt{n}\).

**Proof**

Since \(n\) is composite, it will have at least one prime divisor \(f\).

Let \(n = mp\).

If \(P > \sqrt{n}\) then

\[ n = mp \text{ shows that } \]

\[ m \leq \sqrt{n} \leq P, \]

i.e., there exists a divisor \(m\) of \(n\) less than the least prime divisor, which is contradictory.

Hence, \(P \leq \sqrt{n}\)
Def.
A polynomial congruence
\[ f(x) \equiv 0 \pmod{m} \]
of
\[ f(a) \equiv 0 \pmod{m}. \]

(factor theorem)
A polynomial congruence
\[ f(x) \equiv 0 \pmod{m} \]
has
solution
\[ x \equiv a \pmod{m} \]
if there is a polynomial congruence \( g(x) \) with integral coefficient such that
\[ f(x) \equiv g(x)(x-a) \pmod{m} \]

Proof.
Let \( x \equiv a \pmod{m} \) is
solution of \( f(x) \equiv 0 \pmod{m} \).
Now dividing by \( x-a \) we obtained a polynomial \( g(x) \)
with integral coefficient and
remainder \( r \) s.t.
\[ f(x) \equiv (x-a)g(x) + r \pmod{m} \]
Now \( x \equiv a \pmod{m} \) is solution of
\[ f(x) \equiv 0 \pmod{m} \]
\[ \implies f(a) \equiv 0 \pmod{m}. \]
\[ f(a) = (a-a)q(a) + r \pmod{m} \]
\[ \Rightarrow 0 \equiv 0 + r \pmod{m} \]
\[ \Rightarrow 0 = r \pmod{m} \]

So using \( m \) \( \text{eq.} \( \text{eq.} \)

\[ f(x) = q(x)(a-a) \pmod{m} \]

Conversely

\[ f(x) = q(x)(x-a) \pmod{m} \]

Then

\[ \exists \ x = a \pmod{m} \]

\[ \Rightarrow f(a) = q(a)(a-a) \pmod{m} \]

\[ \Rightarrow f(a) = 0 \pmod{m} \]

\[ \Rightarrow x = a \pmod{m} \]

If \( f(x) = 0 \pmod{m} \) by definition

If

\[ f(x) = a_0 x^n + a_{n-1} x^{n-1} + \cdots + a_0 \]

\[ g(x) = b_0 x^m + b_{m-1} x^{m-1} + \cdots + b_0 \]

are polynomials of degree \( n \) and \( m \) respectively.

Then

\[ f(x) \equiv g(x) \pmod{m} \]

Then

\[ a_i \equiv b_i \pmod{m} \]

for \( i = 1, 2, 3, \ldots, n \).
Let p a prime

Then a congruence \( f(x) \equiv 0 \pmod{p} \)

of degree \( n \) has at most \( n \) solution.

\[ a \equiv b \pmod{p} \]

of degree one has exactly one solution.

Suppose the theorem is true for a congruence of degree \( n-1 \), i.e., a congruence of degree \( n-1 \) has at most \( n-1 \) solution.

Now if \( x \equiv a \pmod{p} \) is a solution of the congruence of degree \( n \). Then by factor theorem

\[ f(x) \equiv (n-a) f(a) \pmod{p} \]

where \( f(a) \) is of degree \( n-1 \).

Therefore the congruence \( f(x) \equiv 0 \pmod{p} \)

has at most \( n-1 \) solutions. (By hypothesis)

Let \( c_1, c_2, \ldots, c_{n-1} \) be the solutions of \( f(x) \).

i.e. \( f(x) \equiv 0 \pmod{p} \).

Now if \( x \equiv c \pmod{p} \) is an any solution of the congruence

\[ f(x) \equiv 0 \pmod{p} \]

\( \Rightarrow f(c) \equiv 0 \pmod{p} \).
using in \( \text{1} \)

\[(c - a) \equiv 0 \pmod{P} \]

either

\[c - a \equiv 0 \pmod{P} \]

or

\[q(c) \equiv 0 \pmod{P} \]

\[c - a \equiv 0 \pmod{P} \]

\[c \equiv a \pmod{P} \]

Now

\[q(c) \equiv 0 \pmod{P} \]

\[x = c \pmod{P} \] is solution of

\[q(x) \equiv 0 \pmod{P} \]

\[c \equiv c_i \pmod{P} \]

for some \( i = 1, 2, 3, \ldots, n - 1 \)

\[c \in \{a, c_1, c_2, c_3, \ldots, c_{n-1}\} \]

\[f(x) \equiv 0 \pmod{P} \] has

at most \( n \) solutions,
Let $p$ be an odd prime
Then the congruence $x^{p-1} \equiv 1 \pmod{p}$ has
exactly $p-1$ solution.

Proof. By Fermat's theorem
\[ a^{p-1} - 1 \equiv 0 \pmod{p} \]
so the congruence
\[ x^{p-1} - 1 \equiv 0 \pmod{p} \]
is satisfied by all the integer
$1, 2, 3, \ldots, p-1$.

Hence all the $p-1$ integers are the solution of
\[ x^{p-1} - 1 \equiv 0 \pmod{p} \]
but by Lagrange's theorem a congruence
of degree $p-1$ has at most $p-1$ solution.

\[ \sum_{\text{all } x} f(x) \equiv (p-1) f(x) \pmod{p} \]
\[ n^2 + n + 1 \equiv 0 \pmod{7} \]

C.R.S of 7 = \{0, 1, 2, 3, 4, 5, 6\} \Rightarrow \{0, 1, 4, 2, 3\}

Hence only solution are

\[ x \equiv 2 \pmod{7} \]

\[ x \equiv 4 \pmod{7} \]

\[ \text{By putting } 2, 4 \text{ in } x^2 + x + 1 \text{ respectively, satisfied.} \]

\[ n^2 + 4n + 2 \equiv 0 \pmod{23} \]

\[ n^2 + 4n + 2 + 2 \equiv 2 \pmod{23} \]

\[ (n+2)^2 \equiv 2 \pmod{23} \]

\[ \Rightarrow (n+2)^2 \equiv 25 \pmod{23} \]

\[ \Rightarrow (n+2) \equiv 5 \pmod{23} \]

\[ \Rightarrow n+2 \equiv 5 \pmod{23} \]

\[ n+2 \equiv 5 \pmod{23} \quad \& \quad n+2 \equiv -5 \pmod{23} \]

\[ n \equiv 8 \pmod{23} \quad \& \quad n \equiv -7 \pmod{23} \]

\[ \Rightarrow n \equiv 16 \pmod{23} \]

Hence the solution set is

\[ \{16, 16 + 23k\} \]
Find all solutions of the congruence

\[ x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod{30} \]

\[ 30 = 2 \cdot 3 \cdot 5 \]

Therefore the given congruence is equivalent to the system of congruences

\[ x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod{2} \] (1)

\[ x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod{3} \] (2)

\[ x^3 - 4x^2 + 15x - 6 \equiv 0 \pmod{5} \] (3)

\[ (i) \Rightarrow (ii) \]

[Redact: x divides \( x^3 + x \) so \( x \equiv 0 \pmod{2} \).]

\[ x \equiv 0 \pmod{2} \]

\[ x \equiv 1 \pmod{2} \] (4)

\[ x \equiv 0 \pmod{3} \]

\[ x \equiv 1 \pmod{3} \]

Now
\[ eq \ 3 \Rightarrow x^3 + x^2 + 4 = 0 \pmod{5} \]

\[ x = 3 \pmod{5} \]

The possible combinations are

a) \( x = 0 \pmod{2} \)
   \[ x = 0 \pmod{3} \]
   \[ x = 3 \pmod{3} \]

b) \( x = 0 \pmod{2} \)
   \[ x = 1 \pmod{3} \]
   \[ x = 3 \pmod{5} \]

c) \( x = 1 \pmod{2} \)
   \[ x = 0 \pmod{3} \]
   \[ x = 3 \pmod{5} \]

d) \( x = 1 \pmod{2} \)
   \[ x = 1 \pmod{5} \]
   \[ x = 2 \pmod{5} \]
a) \[ x \equiv 0 \pmod{2} \]
\[ x \equiv 0 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]

By the Chinese Remainder Theorem

\[ M_1 = \frac{2 \cdot 3 \cdot 5}{2} = 15 \]
\[ M_2 = \frac{2 \cdot 3 \cdot 5}{3} = 10 \]
\[ M_3 = \frac{2 \cdot 3 \cdot 5}{5} = 6 \]

Now

\[ 15y_1 \equiv 1 \pmod{2} \]
\[ 10y_2 \equiv 1 \pmod{3} \]
\[ 6y_3 \equiv 1 \pmod{5} \]

Since

\[ 15y_1 \equiv 0 \pmod{2} \]

\[ 15y_1 - 2uy_2 = 0 \]
\[ (7 \cdot 2y_1 + y_1) - 2uy_2 = 0 \]
\[ 2y + y_1 = 0 \text{ where } 7y_1 - 2uy_2 = y_1 \]
\[ y_1 = -2, \quad y_1 = 1 \]

- \[ y_1 \equiv 0 \pmod{2} \]
\[ y_1 \equiv 0 \pmod{2} \]
\[ 10y_2 \equiv 0 \pmod{a + b} \]

\[ y_2 \equiv 3 \pmod{a + b} \]

Since \[ 0 \equiv 3 \pmod{a + b} \]

\[ y_2 \equiv 0 \pmod{a + b} \]

\[ 6y_3 - 3u_1 = 5 \]
\[ 2y_3 - 3u_1 = 5 \]
\[ 3(2y_3 - u_1) = 5 \]

\[ x = a + y_2 = c \]
\[ (a, b) \mid c \]

\[ (2, 3) = 215 \]

\[ y_1 = 1, \quad y_2 = 1, \quad y_3 = 1 \quad \Rightarrow \quad ? \]

\[ y = M_1 y_1 C_1 + M_2 y_2 C_2 + M_3 y_3 C_3 \]

\[ = (5)(1)(1) + 10(1)(0) + 6(3)(5) \]

\[ = 60 + 30 \equiv 0 \pmod{30} \]

\[ y = 0 \pmod{30} \]
b) \[ \begin{align*} x & \equiv 0 \pmod{2} \\ x & \equiv 1 \pmod{3} \\ x & \equiv 3 \pmod{5} \end{align*} \]

\[ M_1 = \frac{2 \cdot 3 \cdot 5}{2} = 15 \]

\[ M_2 = 10 \]

\[ M_3 = 6 \]

\[ M_1 y_1 = 1 \pmod{15} \]

\[ 15 y_1 = 1 \pmod{2} \]

\[ y_1 = 1 \cdot \]

\[ 10 y_2 = 1 \pmod{3} \]

\[ y_2 = 1 \]

\[ 6 y_3 = 3 \pmod{3} \]

\[ y_3 = 1 \]

\[ y = (15)(1)(0) + (10)(1)(1) + 6(1)(3) \]

\[ = 0 + 10 + 18 \]

\[ y = 28 \]

\[ y \equiv -2 \pmod{30} \]

\[ -2 \equiv 28 \pmod{30} \]

\[ y \equiv 28 \pmod{30} \]
c) \( x = 1 \pmod{2} \\
    x = 0 \pmod{3} \\
    x = 3 \pmod{5} \\
M_1 = 15, \ M_2 = 10, \ M_3 = 6 \\\n\( y_1 = 1, \ y_2 = 1, \ y_3 = 1 \)
\[
\begin{align*}
y &= 15(1)(1) + 10(1)(0) + 6(1)(3) \\
   &= 15 + 0 + 18 \\
   &= 33 \end{align*}
\]
\( \Box \)
\( Y = 3 \pmod{30} \)

d) \( y = 1 \pmod{2} \\
    y = 1 \pmod{3} \\
    y = 3 \pmod{5} \\
M_1 = 15, \ M_2 = 10, \ M_3 = 6 \\\n\( y_1 = 1, \ y_2 = 1, \ y_3 = 1 \)
\( \ell_1 = 1, \ \ell_2 = 0, \ \ell_3 = 3 \)
\[
\begin{align*}
y &= 15 + 10 + 18 \\
   &= 43 \end{align*}
\]
\( \Box \)
\( Y = 43 \pmod{30} \)
We first have:
\[ x^3 - 4x^2 + 5a - 6 \equiv 0 \pmod{3}. \]

Let \( x = 3t \). We find that the only solution is \( t = 0 \pmod{3} \).

Let \( x = 3t \).
\[
(t^3)^3 - 4(t^3)^2 + 5(t^3) - 6 = \equiv (3^2)
\]
\[
9t^3 - 12t^2 + 15t - 6 \equiv \pmod{(3^2)}
\]

Let \( t = 0 \pmod{3} \).
\[
15t - 6 \equiv \pmod{3^2}
\]

Let \( t = 2 \pmod{3} \).
\[
5t \equiv 2 \pmod{3}
\]

This congruence has unique solution \( t = 1 \pmod{3} \).

Let \( t = 1 + 3s \) so that \( t = 1 + 3s \).

\( s = 3 + 9s \) is also of the form.

Congruence:
\[ x^3 - 4x^2 + 5a - 6 \equiv 0 \pmod{3^3} \]

Substituting \( x = 3 + 9s \).

\[ 72s \equiv 0 \pmod{271} \]

\[ 72s \equiv 0 \pmod{271} \]

\[ s \equiv 0 \pmod{271} \]

\[ s = 3 \pmod{27} \]

Hence the given solution of the congruence:
\[ x = 3 + 27s \]
C.R.S of \( y = 2 \)

\[
\begin{align*}
& \lambda = 3 \pmod{5} \checkmark \\
& \lambda = 4 \pmod{5} \checkmark \\
& \lambda = 6 \pmod{7} \\
& \lambda = 5 \pmod{7}.
\end{align*}
\]

The possible combinations are:

a) \( \lambda = 3 \pmod{5} \)

b) \( \lambda = 4 \pmod{5} \)

c) \( \lambda = 3 \pmod{5} \)

d) \( \lambda = 4 \pmod{5} \)
a) \[ x = 3 \pmod{5} \]
\[ x = 5 \pmod{7} \]
\[ M_1 \equiv 7, \quad M_2 \equiv 5. \]
\[ y_1 = 1 \pmod{5} \]
\[ y_2 = 3 \pmod{5} \]
\[ 5y_2 = 1 \pmod{7} \]
\[ y_2 = 3 \pmod{7} \]

\[ y = M_1y_1c_1 + M_2y_2c_2 \]
\[ = (7)(3)(3) + (5)(3)(5) \]
\[ = 63 + 75 \]
\[ y = 138 \]

\[ y = 33 \pmod{35}, \checkmark \]

b) \[ a = 4 \pmod{5} \]
\[ a = 6 \pmod{7} \]
\[ y_1 = 3, \quad y_2 = 3, \quad M_1 \equiv 7, \quad M_2 \equiv 5 \]
\[ y = 84 + 90 \]
\[ y = 174 \]
\[ y = 34 \pmod{35} \]

e) \[ \alpha = 3 \pmod{5} \]
\[ \alpha = 6 \pmod{7} \]
\[ y_1 = 3, \quad y_2 = 3 \]
\[ M_1 = 7, \quad M_2 = 5 \]
\[ c_1 = 3, \quad c_2 = 6 \]
\[ y = 63 + 90 \]
\[ y = 153 \]
\[ y = 13 \pmod{35} \]

d) \[ \alpha = 4 \pmod{5} \]
\[ \alpha = 5 \pmod{7} \]
\[ y_1 = 3, \quad y_2 = 3 \]
\[ M_1 = 7, \quad M_2 = 5 \]
\[ c_1 = 4, \quad c_2 = 5 \]
\[ y = 84 + 75 = 159 \]
\[ y = 19 \pmod{35} \]
\[(p-1)! \equiv -1 \pmod{p}\]

If \(p\) is an odd prime.

Proof: we know that the congruence

\[x^{p-1} - 1 \equiv 0 \pmod{p}\]

has \(p-1\) solutions which are given by

\[x \equiv 1, 2, 3, \ldots, p-1 \pmod{p}\]

if \(p\) is an odd prime. Then by the Factor Theorem:

\[x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\ldots(x-(p-1)) \pmod{p}\]

As both polynomials of degree \(p-1\) are congruent, the constant term on both sides will be congruent \(\pmod{p}\).

\[\equiv -1 \equiv (-1)(-2)(-3)\ldots(-1)^{p-1} \pmod{p}\]

\[\equiv -1 \equiv (-1)^{p-1} \left[ 1 \cdot 2 \cdot 3 \ldots (p-1) \right] \pmod{p}\]

\[\equiv -1 \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}\]

\[\equiv -1 \equiv (p-1)! \pmod{p}\]

\[\iff (p-1)! \equiv -1 \pmod{p}\]

as \(p\) is an odd prime.
Conversely suppose that
$(p-1)! \equiv -1 \pmod{p}$ and $p$ is composite.
Then $7$ an integer $m_1, m_2$ i.e.

$$1 < m_1, m_2 < p$$

so

$$p = m_1 m_2.$$ 

Then

$$(p-1)! \equiv -1 \pmod{m_1 m_2} \implies p = m_1 m_2.$$ 

Now

$$1 < m_1 < p \implies m_1 < p-1.$$ 

So

$$m_1 \mid (p-1)!.$$ 

which is a contradiction hence $p$ must

be prime.

$$\frac{4!}{10} = \frac{10!}{2 \cdot 5} = 2 \cdot 10 - 1 = 9,$$ 

which is a contradiction hence $p$ must

be prime.
order of an integer \((\text{mod } m)\)

\(\text{ord}_m(a) = n\)

if \((a, m) = 1\) and \(a^n \equiv 1 \pmod{m}\)

where \(n\) is the least positive integer for which the congruence is true. Then we say \(a\) belongs to \(\mathbb{Z}_m^*\) \((\text{mod } m)\) or \(a\) has order \(n\) \((\text{mod } m)\).

We can write \(\text{ord}_m(a) = n\).

Note: By Euler's Theorem we know that if \((a, m) = 1\) then

\[a^\phi(m) \equiv 1 \pmod{m}.
\]

It means order of \(a\) \((\text{mod } m)\) always exist, and will less than or equal to \(\phi(m)\).

Proof:

Since \(\text{ord}_m(a) = n\)

\[a^n \equiv 1 \pmod{m}.
\]

\(n\) is least positive integer for which the congruence is true.
Suppose that 
\[ a^r \equiv 1 \pmod{m} \]
and also suppose that 
\[ x = ny + r \quad \text{where} \quad 0 \leq r < n. \]

Now 
\[ a^r \equiv 1 \pmod{m} \]

\[ \Rightarrow a^{ny} \cdot a^r \equiv 1 \pmod{m} \]

\[ \Rightarrow (a^m)^y \cdot a^r \equiv 1 \pmod{m} \]

\[ \Rightarrow a^r \equiv 1 \pmod{m} \quad \text{as} \quad ny < n \quad \text{which is not possible as} \quad n \quad \text{is least positive integer} \]

\[ \Rightarrow r \quad \text{must be equal to zero} \]

So eq (c) becomes

\[ x = ny + 0 \quad \Rightarrow x = 0 \]

\[ \Rightarrow x = ny \]

\[ \Rightarrow \quad a^x \quad \text{which is required.} \]

Conversely, suppose that 
\[ \frac{a^x}{m} \quad \text{and we have prove that} \]
\[ a^k = 1 \pmod{m} \]

since
\[ a^n = 1 \pmod{m} \]
as \( \text{ord}_m(a) = n \).

now
\[ a^n = 1 \pmod{m} \]

\[ (a^n)^y = 1 \pmod{m} \]

\[ a^{ny} = 1 \pmod{m} \]

\[ a^y = 1 \pmod{m} \]

which is required result.

\[ \text{of ord}_m(a) = n \text{ then } n \mid q(m) \]

\[ \text{since ord}_m(a) = n \]

\[ a^n = 1 \pmod{m} \]

Thus, \( n \) is least positive integer, for which the congruence is true.
Also by Euler's Theorem
\[ \phi(a, m) = 1 \text{ then } q(n) \equiv 1 \pmod{m}. \]
But
\[ a^n \equiv 1 \pmod{m}, \]
i.e. \( n \) is the order of \( a \) and hence
\[ n \mid \phi(m). \]

If \( \phi(a, m) = 1 \) \( \Rightarrow \) \( \text{ord}_m(a) = n \)

Then for positive integers \( i \) and \( j \)

\[ a^i \equiv a^j \pmod{m} \]

\[ i = j \pmod{m}. \]

\[ i \geq j, \text{ then } a^i \equiv a^j \pmod{m}. \]

Proof: Suppose
\[ a^i \equiv a^j \pmod{m}. \]

If \( i > j \) then
\[ a \cdot a \cdot a \cdot a \cdots a = a \cdot a \cdot a \cdots a \pmod{m}, \]
\( i \text{ times} \) \( \pmod{m} \)
\( j \text{ times} \)

Since \( (a, m) = 1 \) therefore

\[ i - j \]

\[ a^i \equiv 1 \pmod{m}. \]

but
\[ a^n \equiv 1 \pmod{m}. \]

\[ \Rightarrow n \mid i - j \]
\[ i - j \equiv 0 \pmod{n} \Rightarrow i \equiv j \pmod{n} \]

Conversely, suppose that \[ i \equiv j \pmod{n} \]

Then \[ i - j \equiv 0 \pmod{n} \]

Then \[ m \mid i - j \]

Then \[ j \in \mathbb{Z} \text{ s.t.} \]

\[ i - j = nz \]

Then \[ i = j + nz \]

Since \[ a^0 = a^i \pmod{m} \]

Then \[ a^i = a^{i+nz} = a^{(a^n)^z} \pmod{m} \]

\[ a^i \equiv a^j \pmod{m} \]

which is required result.
i) \(a \equiv b \pmod{m}\) \\
Then \\
\(\text{ord}_m(a) = \text{ord}_m(b)\) \\
ii) \(ab \equiv 1 \pmod{m}\) \\
Then \\
\(\text{ord}_m(a) = \text{ord}_m(b)\)

Proof

Suppose \(\text{ord}_m(a) = n_1\) and \(\text{ord}_m(b) = n_2\)

\[
\Rightarrow a^{n_1} \equiv 1 \pmod{m}
\]
and
\[
b^{n_2} \equiv 1 \pmod{m}.
\]

Since
\[
a \equiv b \pmod{m}
\]

\[
\Rightarrow a^{n_1} \equiv b^{n_1} \pmod{m}.
\]

\[
\Rightarrow 1 \equiv b^{n_1} \pmod{m}.
\]

so
\[
b^{n_1} \equiv 1 \pmod{m} \text{ by symmetry}
\]

But 
\[
b^{n_2} \equiv 1 \pmod{m} \text{ congruent}
\]

\[
\Rightarrow n_2 | n_1 \implies \text{ord}_m b = n_2.
\]

Now
\[
a^{n_2} \equiv b^{n_2} \pmod{m}
\]

\[
\Rightarrow a^{n_2} \equiv 1 \pmod{m} \implies b^{n_2} \equiv 1 \pmod{m}.
\]
\[ \text{If } ab \equiv 1 \pmod{m} \]
\[ \text{Then } \text{ord}_m(a) = \text{ord}_m(b) \]

**Proof:** Suppose \[ \text{ord}_m(a) = n_1 \]
\[ \text{ord}_m(b) = n_2 \]

\[ \Rightarrow a^{n_1} \equiv 1 \pmod{m} \]
\[ b^{n_2} \equiv 1 \pmod{m} \]

Since
\[ ab \equiv 1 \pmod{m} \]

\[ \Rightarrow (ab)^{n_1} \equiv 1 \pmod{m} \]

\[ \Rightarrow a^{n_1}b^{n_1} \equiv 1 \pmod{m} \]

\[ \Rightarrow b^{n_1} \equiv 1 \pmod{m} \]
But \( \text{ord } (b) = n_2 \)

\[ \Rightarrow \quad m_2 \mid m_1 \quad (1) \]

Now

\[ (ab)^{m_2} = 1^{m_2} \quad (\text{mod } m) \]

\[ a^{m_2}b^{m_2} = 1 \quad (\text{mod } m) \]

\[ a^{m_2} = 1 \quad (\text{mod } m) \quad \Rightarrow \quad b^{m_2} = 1 \quad (\text{mod } m) \]

But

\[ \text{ord } (a) = n_1 \]

\[ \Rightarrow \quad m_1 \mid m_2 \quad (2) \]

From (1) & (2) we have

\[ m_1 = m_2 \]

\[ \text{ord } (a^2) = \text{ord } (b) \]

If \((s,t)=1 \) and \( a' \) belongs to \( S' \quad (\text{mod } m) \) and \( b' \) belongs to \( t' \quad (\text{mod } m) \). Then \( ab \) belongs to \( st' \quad (\text{mod } m) \).

Proof

we know

\[ a^s \equiv 1 \quad (\text{mod } m) \]

\[ b^t \equiv 1 \quad (\text{mod } m) \]
\[ \text{if } \text{ord}_m(ab) = k \]

\[ \Rightarrow (ab)^k \equiv 1 \pmod{m} \]

Now as

\[ a^k \equiv 1 \pmod{m} \]

\[ \Rightarrow a^t \equiv 1 \pmod{m} \quad \text{--- (1)} \]

also \[ b^t \equiv 1 \pmod{m} \]

\[ b^k \equiv 1 \pmod{m} \quad \text{--- (2)} \]

Multiplying eqn 1 \& 2, we get

\[ a^k b^t \equiv 1 \pmod{m} \]

\[ \Rightarrow \text{ord}_m(ab) = k \text{ \& } (ab)^k \equiv 1 \pmod{m} \]

\[ \Rightarrow k \mid st \quad \text{--- (3)} \]

Next

\[ (ab)^k \equiv 1 \pmod{m} \]

\[ a^k b^k \equiv 1 \pmod{m} \]

\[ (a^k b^k)^t \equiv 1 \pmod{m} \]

\[ a^{kt} b^{kt} \equiv 1 \pmod{m} \]
\[
\Rightarrow a^{\text{ord}_m(b)} = 1 \quad \text{(mod } m) \quad \Rightarrow \quad b^t = 1 \quad \text{(mod } m) \\
\quad \text{But} \\
\text{ord}_m(a) = \sigma \quad \Rightarrow \quad a^\sigma = 1 \quad \text{(mod } m) \quad b^t = 1 \quad \text{(mod } m) \\
\Rightarrow \quad 8^t \equiv 1 \quad \text{(mod } m) \\
\quad \text{Similarly} \\
(ab)^t = 1 \quad \text{(mod } m) \\
(ab)^{\text{ord}_m(b)} = 1 \quad \text{(mod } m) \\
\Rightarrow \quad ab^t \equiv 1 \quad \text{(mod } m) \\
\quad \text{But} \\
\text{ord}_m(b) = t \quad \Rightarrow \quad b^t = 1 \quad \text{(mod } m) \quad a^\text{ord}_m(b) = 1 \quad \text{(mod } m) \\
\Rightarrow \quad t \mid \text{ord}_m(b) \\
\Rightarrow \quad t \mid k \quad \text{for } k \quad \text{(st)} = 1 \\
\Rightarrow \quad \text{st} \mid k - (5) \quad \text{for } (st) = 1 \\
\text{from (3) and (5) we get} \\
\Rightarrow \quad k = \text{st} \\
\Rightarrow \quad \text{ord}_m(ab) = \text{st} \\
\]
when \( (a, m) = 1 \) and \( a \) belongs to \( \varphi(m) \) (ma of m).

Then \( a \) is called a primitive root of \( m \), i.e.

\[
\varphi(m) \equiv a \equiv 1 \pmod{m}
\]

For e.g.,

\[
\begin{align*}
8 & \equiv 1 \pmod{9} \quad \text{1 is primitive root of 1} \\
1 & \equiv 1 \pmod{9} \quad \text{and} \\
2 & \equiv 1 \pmod{9}
\end{align*}
\]

Note: 1 is the primitive root for

Those for which \( \varphi(m) = 1 \) i.e. \( 1^k \).

i) \( 2 \) is a primitive root of 3.

\[
\begin{align*}
8(3) & \equiv 2 \equiv 1 \pmod{3} \\
3 & \equiv 1 \pmod{4} \quad \text{2 is the primitive root of 4.}
\end{align*}
\]

The only integers which have

primitive roots are

1. \( 1, 2, 4, p^n \) and \( 2p^n \) where

\( p \) is an odd prime

2. \( 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, p^n \) and \( 2p^n \).
If \( \phi(m) \) has primitive root \( q \), then \( \phi(n) \) has \( \phi(q^m) \) primitive roots given by

\[
1 \leq x \leq \phi(q^m) - 1, \quad (x, \phi(q^m)) = 1
\]

denoted by \( \sigma_q \).

For e.g., for 13

\[
\phi(13) = 12: \quad 13 \text{ is odd}
\]

\[
\phi(q(13)) = \phi(12) = \frac{12}{(1 - \frac{1}{p}) (2 - 13)} \quad q(m) = m - 1
\]

\[
= 12 \left(1 - \frac{1}{2}\right) (12 - 13) = 12 \left(\frac{1}{2}\right) (\frac{1}{13}) = 4
\]

\[
(1, 12) = 1
\]

\[
(5, 12) = 1
\]

\[
(7, 12) = 1
\]

\[
(11, 12) = 1
\]
Find all primitive roots

$\phi(17) = 16$; 17 is odd prime.

$(2, 17) = 1$

$2^1 \equiv 2 \pmod{17}$

$2^2 \equiv 4 \pmod{17}$

$2^3 \equiv 8 \pmod{17}$

$2^4 \equiv 16 \pmod{17}$ or $2^4 \equiv -1 \pmod{17}$

$2^5 \equiv -2 \pmod{17}$

$2^6 \equiv -4 \pmod{17}$

$2^7 \equiv -8 \pmod{17}$

$2^8 \equiv -16 \pmod{17}$

$2^8 \equiv 1 \pmod{17}$ or $-16 \equiv 1 \pmod{17}$

So 2 is not primitive root of 17.

Now

$(3, 17) = 1$

$3^1 \equiv 3 \pmod{17}$. 
$3^2 = 9 \pmod{17}$

$3^3 = 10 \pmod{17}$

$3^4 = 13 \pmod{17}$

$3^5 = 5 \pmod{17}$

$3^6 = 15 \pmod{17}$

$3^7 = 11 \pmod{17}$

$3^8 = -1 \pmod{17}$

$\varphi(17) = \frac{16 \cdot 17 - 17}{17} = 15 \equiv 1 \pmod{17}$

$3 = 3^6 = 1 \pmod{17}$

3 is primitive root of 17 by definition.

Now $q(q(17)) = q(16) = 16 (1 - \frac{1}{2}) = 8 = 2^3$.

$q(q(17)) = 8^1$.

So it has 8 numbers (primitive) roots.

Now $1 \leq \alpha \leq 16 - 1$ implies $1 \leq \alpha \leq 15$.

Such $\alpha$'s are $(\alpha, 16) = 1$.
\[(1, 16) = 1\]
\[(3, 16) = 1\]
\[(5, 16) = 1\]
\[(7, 16) = 1\]
\[(9, 16) = 1\]
\[(11, 16) = 1\]
\[(13, 16) = 1\]
\[(15, 16) = 1\]

All primitive roots of 17 given by \(g^a\):

\[3, 3, 3, 3, 3, 3, 3, 3\]

Find all primitive roots of 11, 13, 15, and 19.

**Solution:**

\[\begin{align*}
q(19) &= 18 \\
(2, 19) &= 1 \\
9 &= 2 \mod (19) \\
2^3 &= 6 \mod (19) \\
2^3 &= 8 \mod (19)
\end{align*}\]
\[2^4 \equiv 16 \ (\text{mod} \ 19)\]
\[2^5 \equiv 13 \ (\text{mod} \ 19)\]
\[2^6 \equiv 7 \ (\text{mod} \ 19)\]
\[2^7 \equiv 14 \ (\text{mod} \ 19)\]
\[2^8 \equiv 9 \ (\text{mod} \ 19)\]
\[2^9 \equiv 18 \ (\text{mod} \ 19)\]
also \[2^9 \equiv -1 \ (\text{mod} \ 19)\]
\[2^{48} \equiv 1 \ (\text{mod} \ 19)\]

\[\Rightarrow 2 \text{ is the primitive root} \ (\text{mod} \ 19)\]

Now \[\varphi (19) = 18\]
\[\varphi (18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6\]

\[\varphi (19) = 6 \text{ where } (a, 6) = 1, \ 1 \leq a \leq \varphi(19) - 1 = 18 - 1 = 17\]

such \(a\)'s which are \((a, 18) = 1\):

\[(1, 18), \ (5, 18) = 1, \ (13, 18) = 1, \ (11, 18) = 1\]
So all the primitive roots of 19 is given by $\alpha^g$.

i.e. $1, 5, 7, 11, 13, 17$. 

\[ x \equiv 0 \pmod{2} \quad (i) \]
\[ x \equiv 0 \pmod{3} \quad (ii) \]
\[ x \equiv 3 \pmod{5} \quad (iii) \]

Solution

B2. $x \equiv 0 \pmod{2}$

\[ x = 0 + 2h \]

\[ x = 2h \quad (iv) \]

Using in (ii)

\[ 2h \equiv 0 \pmod{3} \]

\[ h \equiv 0 \pmod{3} \quad ; (2, 3) = 1 \]

\[ h = 0 + 38 \quad \text{for } \mathbb{Z}, \]

\[ h = 38 \]
\(\text{egn (3) } \Rightarrow \alpha = 6 \left(3 + 5t\right)\)

\(\alpha = 18 + 30t\)

\(\alpha = 18 \pmod{30} \Rightarrow 30t = 0 \pmod{30}\)

If \(P_1\) and \(P_2\) are odd prime and

\[m = a_1 \pmod{d_1}, m = a_2 \pmod{d_2}\]

Moreover, if \(a_1\) belongs to \(d_1 \pmod{d_2}\), then

\(m\) belongs to least common multiple of \(d_1\) and \(d_2\) \(\pmod{d_2}\).

\(\text{Proof:}\) let \(L = \langle d_1, d_2 \rangle = \text{l.c.m. of } d_1, d_2\)

Also, given that

\[a_1 \equiv 1 \pmod{d_1}\]

\[a_2 \equiv 1 \pmod{d_2}\].
\[ (a_1)^2 \equiv 1 \mod p_1 \]

and

\[ (a_2)^2 \equiv 1 \mod p_2 \]

\[ \Rightarrow a_1 \equiv 1 \mod p_1 \]

\[ a_2 \equiv 1 \mod p_2 \]

Then

\[ m^2 \equiv a_1 \equiv 1 \mod p_1 \]

i.e.

\[ m^2 \equiv 1 \mod p_1 \]

also

\[ m^2 \equiv a_2 \equiv 1 \mod p_2 \]

i.e.

\[ m^2 \equiv 1 \mod p_2 \]

\[ \Rightarrow p_1 \mid m^2 - 1 \quad \& \quad p_2 \mid m^2 - 1 \]

\[ \Rightarrow p_1 p_2 \mid m^2 - 1 \quad \Rightarrow (p_1 p_2) \mid m^2 - 1 \]

\[ m^2 \equiv 1 \mod p_1 p_2 \]

now if \( m \) belongs to \( \mathbb{Z} \mod p_1 p_2 \)

Then

\[ m^k \equiv 1 \mod p_1 p_2 \]
Then
\[ m^k \equiv 1 \pmod{p_1 p_2} \]
\[ \Rightarrow m^k \equiv 1 \pmod{p_1} \]
\[ m^k \equiv 1 \pmod{p_2} \quad ; \quad (p_1, p_2) = 1 \]
Also
\[ m d_1 \equiv a_1 \equiv 1 \pmod{p_1} \]
\[ \Rightarrow m d_1 \equiv 1 \pmod{p_1} \]
\[ \text{(similarly) } m d_2 \equiv a_2 d_2 \equiv 1 \pmod{p_2} \]
\[ m d_2 \equiv 1 \pmod{p_2} \].
\[ \Rightarrow d_1 | \ell \text{ and } d_2 | \mu. \]
\[ \Rightarrow \ell \text{ is common multiple of } d_1, d_2 \text{ but } \langle d_1, d_2 \rangle = 1. \]
\[ \frac{\ell}{2} | \mu \rightarrow 2 \]
From 0 and 2
\[ K = L \]
\[ \text{i.e. } m \ell \equiv 1 \pmod{p_1 p_2} \]
\[ \Rightarrow m \ell \text{ belongs to } L \pmod{p_1 p_2} \]
Let \( p \) be an odd prime and \( \gamma \) is a primitive root of \( p \). Then

\[ \eta \equiv \gamma^k \pmod{p} \]

the exponent \( \eta \) is called index of \( \eta \) (mod \( p \)) relative to base \( \gamma \).

i.e.

\[ \eta = \text{index}_\gamma \eta \]

\[ \eta \equiv \gamma^k \pmod{p} \]

\[ \eta \equiv \gamma^t \pmod{p} \]

\( \eta \) and \( \gamma \) are relatively prime.

Proof: Let \( \gamma \) be the primitive root of \( p \). Let

\[ \text{index}_\gamma \eta = k \]

\[ \text{index}_\gamma \eta = t \]

\[ \Rightarrow \eta \equiv \gamma^k \pmod{p} \]

\[ \eta \equiv \gamma^t \pmod{p} \]

Suppose \( k > t \).
\[ x^s \cdot \overline{x}^t \equiv \overline{x}^s \cdot x^t \pmod{p} \]

\[ x^s = \overline{x}^t \pmod{m - 1} \]

\[ \Rightarrow x^s = 1 \pmod{m - 1} \]

But by definition,
\[ \phi(m) = \frac{m}{\gcd(m, n)} \]

\[ 2 \cdot \overline{x}^s \cdot \overline{x}^t = \overline{x}^{s + t} \]

\[ \overline{x}^{s + t} = 1 \pmod{m - 1} \]

\[ \Rightarrow s + t \equiv 1 \pmod{m - 1} \]

\[ s = t \pmod{m - 1} \]

\[ m \equiv n \pmod{m - 1} \]

\[ \Rightarrow \text{ind}_x^m \equiv \text{ind}_y^m \pmod{(m - 1)} \]

**Proof:** Let \( s \) be the premiun, best of \( p \) and \( q \), and
\[ \text{ind}_x^m = s \]
\[ \text{ind}_y^m = t \]

\[ \Rightarrow m \equiv x^s \pmod{m - 1} \]
\[ \equiv n \equiv x^t \pmod{m - 1} \]
Now \( m \equiv n \pmod{p} \)

\[ \implies s^g \equiv s^t \pmod{p} \]

\[ \text{and} \quad m^d m \equiv m^d n \pmod{p} \]

\[ \implies b \equiv h \pmod{p} \]

Now suppose \( s > t \)

\[ \implies m^d m - m^d n \]

\[ \implies b \equiv 1 \pmod{p} \]

But \( q(P) \equiv p^{-1} \)

\[ \implies s \equiv s \pmod{p} \]

\[ p^{-1} \mid m^d m - m^d n \]

\[ \implies m^d m \equiv m^d n \pmod{p-1} \]

\[ \therefore \ if \ m \nmid a-b \]

\[ \implies a \equiv b \pmod{m} \]

Conversely suppose that \( m^d m \equiv m^d n \pmod{p-1} \)

By def. of congruence

\[ p^{-1} \mid m^d m - m^d n \]
\[ h \equiv m \cdot m^n \equiv 1 \pmod{p} \]

\[ \Rightarrow \quad m \cdot m^n \equiv 1 \pmod{p} \]

\[ \Rightarrow \quad h \equiv h \pmod{p} \quad \text{if } q(p) \nmid 2. \]

Then

\[ h \equiv h \pmod{p} \]

\[ \Rightarrow \quad h^g \equiv h^t \pmod{p}. \]

\[ h \equiv m \pmod{p} \quad \text{and } \quad h^t \equiv n \pmod{p} \]

Therefore

\[ m \equiv n \pmod{p} \]

If \( g \) is a primitive root of \( q \), and

\[ a \equiv b \pmod{q} \] then

\[ \begin{align*}
\text{(i)} & \quad \text{ind}_g (ab) \equiv \text{ind}_g a + \text{ind}_g (b) \pmod{\phi(q)} \\
\text{(ii)} & \quad \text{ind}_g a^n \equiv n \cdot \text{ind}_g a \pmod{\phi(q)} \end{align*} \]

Proof: Let \( g \) be the primitive root of \( q \).

\[ \text{let } \text{ind}_g (ab) = t \]
\[ ab \equiv g^t \pmod{d^r} \]

Also, suppose that

\[ \text{md}_g a = t_1 \quad \text{and} \]
\[ \text{md}_g b = t_2 \quad \text{and} \]

\[ a \equiv g^{t_1} \pmod{d^r} \quad \text{and} \]
\[ b \equiv g^{t_2} \pmod{d^r} \]

Since

\[ a \equiv b \pmod{d} \]

Therefore

\[ g^{t_1} \equiv g^{t_2} \pmod{d^r} \]

Suppose \( t_1 > t_2 \)

\[ g^{t_1} - g^{t_2} = 1 \pmod{d^r} \]

\[ \Rightarrow g^{t_1 - t_2} \equiv 1 \pmod{d^r} \]

But by definition of primitive

\[ q(g) = 1 \pmod{d^r} \]

So \( q(g) \mid t_1 - t_2 \).
\[ t_1 = t_2 \ (\text{mod} \ q(r)) \]

Now from (1) & (2)

\[ ab = g^{t_1} \cdot g^{t_2} \ (\text{mod} \ q) \]

\[ ab = g^{t_1 + t_2} \ (\text{mod} \ q) \]

\[ g^t = g^{t_1 + t_2} \ (\text{mod} \ q) \]

\[ \Rightarrow ab = t(\text{mod} \ q) \]

\[ \Rightarrow g^{t-t_1+t_2} = 1 \ (\text{mod} \ q) \]

By definition of primitive

\[ g^{\phi(q)} = 1 \ (\text{mod} \ q) \]

\[ \Rightarrow \phi(q) \mid t-t_1+t_2 \]

\[ \Rightarrow t = t_1 + t_2 \ (\text{mod} \ q(r)) \]

\[ \Rightarrow \text{ind}_b ab = \text{ind}_b g + \text{ind}_b b \ (\text{mod} \ q(r)) \]

which is required result.
\[ \text{ind}_a a^n = n \text{ind}_a a \pmod{q(a)} \]

Since

\[ \text{ind}_a a^n = \text{ind}_a (a \cdot a \cdot a \cdots a) \]

\[ = \text{ind}_a a + \text{ind}_a a + \cdots + \text{ind}_a a \pmod{q(a)} \]

\[ \text{ind}_a a^n = n \text{ind}_a a \pmod{q(a)} \]

---

If \( g \) and \( h \) are primitive roots of \( p \), then

\[ \text{ind}_h (a) = \text{ind}_g a \cdot \text{ind}_h (a) \pmod{p-1} \]

\text{Suppose}

\[ \text{ind}_h a = t. \]

\[ \text{ind}_a a = t_1. \]

\[ \text{ind}_g a = t_2. \]

\[ \Rightarrow a = g^{t_1} \pmod{p} \quad (1) \]

\[ a = g^{t_2} \pmod{p} \quad (2) \]
\[ g = h^{t_2} \pmod{d'P} \quad (3) \]

eqn (3) \Rightarrow

\[ g^{t_2} = h^{t_1 t_2} \pmod{d'P} \]

\[ a = h^{t_1 t_2} \pmod{d'P} \]

\[ h^{t_1} = a^{t_1} \pmod{d'P} \]

\[ h^{t_2} \equiv h^t \pmod{d'P} \Rightarrow a = h^{t_2} \pmod{d'P} \]

\[ h^{t_1 t_2 - t} \equiv 1 \pmod{d'P} \]

But by definition, primitive root

\[ h^{t_1} \equiv 1 \pmod{d'P} \]

\[ \Rightarrow h^{t_1 - 1} \equiv 1 \pmod{d'P} \]

\[ \Rightarrow t(t_1 - 1) \]

\[ \Rightarrow t = t_1 \pmod{d'P-1} \]

\[ t \equiv t_1 t_2 \pmod{d'P-1} \]

\[ \text{mdP}a \equiv \text{mdP}a \cdot \text{mdP}8 \pmod{d'P-1} \]
Solve with the help of indices

$$17x \equiv 10 \pmod{29}.$$ 

Since $2$ is the primitive root of $29$, so we have the table for indices:

<table>
<thead>
<tr>
<th>$x$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>3</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{md}a$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>12</th>
<th>18</th>
<th>9</th>
<th>18</th>
<th>7</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{md}a$</td>
<td>7</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>28</th>
<th>29</th>
<th>25</th>
<th>21</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{md}a$</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>26</th>
<th>23</th>
<th>17</th>
<th>5</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{md}a$</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>20</th>
<th>11</th>
<th>22</th>
<th>15</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{md}a$</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
</tbody>
</table>
Now as we know
\[ \text{mod}_g(ab) = \text{mod}_g(a) + \text{mod}_g(b) \mod g^2 \]
Now we have
\[ 17x = 10 \mod 29 \]
\[ \text{mod}_g(17x) = \text{mod}_g 10 \mod 28 \]
\[ \text{md}_g 17 + \text{md}_g x = \text{md}_g 10 \mod 28 \]
\[ \text{md}_g x = \text{md}_g 10 - \text{md}_g 17 \mod 28 \]
\[ = 23 - 21 \mod 28 \]
\[ \text{md}_g x = 2 \mod 28. \]
\[ x = 2 \mod 28 \]
\[ x = 4 \mod 28. \]
which is the required solution of
\[ 17x = 10 \mod 29. \]
Ex:

1. \( 5x^2 \equiv 3 \pmod{11} \)
   \[ 17x^2 \equiv 10 \pmod{29} \]

2. \( \Phi(11) \) \( 5x^2 \equiv 3 \pmod{11} \)

First we find the primitive of 11.

Since \( \Phi(11) = 10 \)

Since \( (2, 11) = 1 \)

and

\[ 2^{10} \equiv 1 \pmod{11} \]

So 2 is the primitive root

2  4  8  5  3  3  5  9  4  1

\( \text{mod} \) 1  2  3  4  5  6  7  8  9  10

Now as we know that,

\[ \text{mod}_{16} = \text{mod}_{2} + \text{mod}_{8} \pmod{40} \]

\[ \text{mod}_{16} = n \cdot \text{mod}_{2} \pmod{40} \]
So we have

\[5x^2 \equiv 8 \quad (\text{mod } 11)\]

\[\Rightarrow \quad m_5 \equiv m_2^{-3} \quad (\text{mod } 10)\]

if \(m = n \quad (\text{mod } p)\)

\[\Rightarrow \quad m_5 + m_2 \equiv m_2^{-3} \quad (\text{mod } 10)\]

\[\Rightarrow \quad m_2 = m_2^{-3} \quad (\text{mod } 10)\]

\[\Rightarrow \quad 3 + 2m_2 \equiv 8 \quad (\text{mod } 10)\]

\[2m_2 \equiv 5 \quad (\text{mod } 10)\]

\[\Rightarrow \quad m_2 \equiv \frac{5}{2} \quad (\text{mod } 10)\]

\[x \equiv \frac{5}{2} \quad (\text{mod } 10)\]

since \(x = \frac{m}{2}\)
If \( x^n \equiv c \pmod{m} \) is solvable and \((m, c) = 1\), then \( c\) is said to be the \( n\)th power residue of \( m\); otherwise \( m\) is said to be non-residue.

If \( x^2 \equiv c \pmod{m} \) is solvable and \((m, c) = 1\), then \( c\) is said to be quadratic residue of \( m\); otherwise \( m\) is quadratic non-residue.

If the congruence has no solution, then \( c^2\) is said to be quadratic non-residue of \( m\).

Example:

\( x^2 = 2 \pmod{7} \) has

\( x = \pm 3 \pmod{7} \) and \((2, 7) = 1\), then \( 2\) is quadratic residue of \( 7\).

This congruence has no solution.

So, \( 2\) is quadratic non-residue of \( 5\).
If \( n \) is quadratic residue of \( m > 2 \) Then
\[
a^2 \equiv 1 \pmod{m}, \quad (a, m) = 1
\]

Proof: Suppose that the congruence
\[x^2 \equiv a \pmod{m}\]
has solution
\[x \equiv \ell \pmod{m}\]
with \((\ell, m) = 1\)
Then by transitive property of congruences
\[\Rightarrow \quad \ell^2 \equiv a \pmod{m}\]
Since \( m > 2 \) so \( \phi(m) \) is even
\[
\phi(m) = \phi(m)
\]
\[\ell^2 \equiv a \pmod{m}\]
\[\ell \equiv a^{\frac{1}{2}} \pmod{m}\]
Now by Euler's Theorem.
Since \((\ell, m) = 1\) so \( \ell^\phi(m) \equiv 1 \pmod{m} \)
Then
\[
eq 1 \equiv \ell^\phi(m) \equiv 1 \pmod{m}
\]

\[10^2 \equiv 1 \pmod{7}
\]
\[8 \equiv 1 \pmod{7}
\]
\[6 \equiv 1 \pmod{7}
\]
So by above method
\[3^3 \equiv 1 \pmod{7}\]
If \( p \) is an odd prime and \( (a, p) = 1 \), we define the Legendre symbol as:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue of } p \text{ and } a \neq 0 \pmod{p} \\
-1 & \text{if } a \text{ is quadratic non-residue of } p \\
0 & \text{if } a = 0 \pmod{p} 
\end{cases}
\]

For example,

\[
\left( \frac{2}{7} \right) = 1 \quad x^2 \equiv 2 \pmod{7} \\
\left( \frac{2}{5} \right) = -1 \quad x^2 \equiv 2 \pmod{5} \quad \text{since } 2 \text{ is quadratic non-residue} \\
\left( \frac{2}{11} \right) = \frac{2}{11} \quad x^2 \equiv 2 \pmod{11}
\]

If \( \left( \frac{2}{p} \right) = 0 \), then \( x^2 \equiv 2 \pmod{p} \) has a solution.
Then \( x^2 = a_2 \pmod{p} \) is also solvable and \( a_2 \) is quadratic residue of \( p \), i.e.

\[
\left( \frac{a_1}{p} \right) = 1 = \left( \frac{a_2}{p} \right)
\]

Similarly if \( a_1 \) is quadratic non-residue then \( a_2 \) is also quadratic non-residue of \( p \), i.e.

\[
\left( \frac{a_1}{p} \right) = -1 = \left( \frac{a_2}{p} \right)
\]

**2)** \( \left( \frac{1}{p} \right) = 1 \). Since \( x^2 = 1 \pmod{p} \)

so \( 1 \) is quadratic residue of \( p \). Thus \( \left( \frac{1}{p} \right) = 1 \) is the solution.

**3)** \( \left( \frac{a^2}{p} \right) = 1 \) if \( \left( a, p \right) = 1 \)

*4) Product of two quadratic residues and two quadratic non-residues is a quadratic residue.*

The product of a quadratic residue with a quadratic non-residue is quadratic non residue, i.e.

\[ a_1, a_2 \text{ are quadratic residues} \]
Then \( \left( \frac{a_1, a_2}{p} \right) = 1 = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right) \)

Similarly

9) \( a_1 \) and \( a_2 \) are non-

quadratic residue.

\( \left( \frac{a_1, a_2}{p} \right) = 1 = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right) \)

Similarly

9) If \( a_1 \) is quadratic and \( a_2 \) is non-quadratic, then

\( \left( \frac{a_1, a_2}{p} \right) = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right) \)

5) \( \left( \frac{a_i}{p} \right) = 1, \quad i = 1, 2, 3, \ldots, n \)

then

\( \left( \frac{a_1, a_2, a_3, \ldots, a_n}{p} \right) = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right) \left( \frac{a_3}{p} \right) \left( \frac{a_n}{p} \right) \)

6) \( \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right) = 1 \)

\( \quad \Rightarrow \left( \frac{a_1}{p} \right) = \left( \frac{a_2}{p} \right) \)

indicates that \( a_1 \) and \( a_2 \), both are residue.

are non-residue.

\( \Rightarrow a_1, a_2 \) have opposite same

quadratic character if both are
Quadratic residue or quadratic non-residue. I have conjectured

\[
\begin{pmatrix} a_1 \\ p \end{pmatrix} \begin{pmatrix} a_2 \\ p \end{pmatrix} = -1
\]

Quadratic character if one is good

\[
\begin{pmatrix} a_1 \\ p \end{pmatrix} = -\begin{pmatrix} a_2 \\ p \end{pmatrix}, \quad \text{if other is quadratic non-residue.}
\]
(1) If \( p \) is a positive odd integer, then
\[
\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}
\]
Quadratic residue. e.g. \( \left( \frac{-1}{211} \right) = (-1)^{\frac{211-1}{2}} \).

(ii) If \( p \) is an odd prime, then
\[
\left( \frac{2}{p} \right) = (-1)^{\frac{p-1}{2}}
\]
in quadratic residue of \( 7 \).

Remark:
The quadratic reciprocity law:
If \( p \) and \( q \) are distinct odd primes, then
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

Show that 33 is the quadratic non-residue of 89.

So:
Since 33 = 3 \times 11
\[
\left( \frac{33}{89} \right) = \left( \frac{3 \times 11}{89} \right)
\]
\[
\left( \frac{33}{89} \right) = \left( \frac{3}{89} \right) \left( \frac{11}{89} \right).
\]

If \( \left( \frac{3}{89} \right) = 1 \) \( \left( \frac{11}{89} \right) = \frac{1}{1} \)
first we take \( 3/89 \).
\[
\begin{align*}
\left( \frac{3}{89} \right) \left( \frac{89}{3} \right) &= (-1)^\frac{89-1}{2} \cdot \frac{3-1}{2} \\
&= (-1)^4 = 1
\end{align*}
\]

Clearly, \( \left( \frac{3}{89} \right) \) and \( \left( \frac{89}{3} \right) \) have the same quadratic character.

So we check \( 89/3 \equiv 2/3 \mod (89) \):

\[
\begin{align*}
\left( \frac{2}{3} \right) &= (-1)^\frac{3-1}{2} \\
&= (-1)^1 = -1
\end{align*}
\]

So \( 3/89 = -1 \).

Similarly, \( \left( \frac{11}{89} \right) \left( \frac{89}{11} \right) \):

\[
\begin{align*}
\left( \frac{11}{89} \right) &= (-1)^\frac{89-1}{2} \\
&= (-1)^4 = 1
\end{align*}
\]

Clearly, \( \left( \frac{11}{89} \right) \) and \( 1-S \left( \frac{89}{11} \right) \) have the same quadratic character.

So we check \( (89/11) \equiv (1/11) \mod (89) \):

\[
\begin{align*}
\left( \frac{11}{89} \right) &= 1 \\
\left( \frac{1}{11} \right) &= 1
\end{align*}
\]

Using these values in \( \left( \frac{33}{89} \right) \):

\[
\begin{align*}
\frac{33}{89} &= (-1) (1) = -1 \\
33 \text{ is quadratic non-residue of } 89.
\end{align*}
\]
4. \((\frac{67}{89})\) is quadratic residue or quadratic non-residue.

\[ 67 \equiv -22 \pmod{89} \]

\[
\left(\frac{-22}{89}\right) = \left(\frac{-1 \cdot 2 \cdot 11}{89}\right)
\]

\[
= \left(\frac{-1}{89}\right) \left(\frac{2}{89}\right) \left(\frac{11}{89}\right)
\]

\[
= \left(-1\right) \left(-1\right) \left(-1\right) = 1
\]

\[
\frac{89-1}{8} \cdot \frac{89^2-1}{8} = \left(-1\right)^{\frac{11-1}{2}} \cdot \left(-1\right)^{\frac{89-1}{8}} = \left(-1\right)^{5.44} = \left(-1\right)
\]

As \(\frac{11}{89}\) and \(\frac{89}{11}\) have same quadratic character

\[
\left(\frac{89}{11}\right) = \left(\frac{11}{89}\right) = 1
\]

So

\[
\left(\frac{11}{89}\right) = 1
\]

\[
eg \Rightarrow \left(\frac{67}{89}\right) = \left(\frac{-22}{89}\right)
\]

\[
= \left(-1\right)^4 \left(-1\right)^{-990} = \left(-1\right)^{990} = 1
\]

\[
\Rightarrow 67 \text{ is quadratic residue of } 89
\]
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = 1
\]

\[\Rightarrow \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \text{ reciprocity property.}\]

If \( p \) and \( q \) are distinct odd primes, then Legendre symbol \( \left( \frac{p}{q} \right) \) will be equal to \( q/p \) unless both \( p \) and \( q \) are of the form \( 4k+1 \) or \( 4k+3 \). In this case,

\[\left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right) .\]

E.g. \[\frac{11}{19} = \frac{4(4)+3}{4(4)+3} = -1 .\]

Assignment:-

182/271
Let \( x \in \mathbb{R} \). Then we define \([x]\), the greatest integer not exceeding \( x\), as the "Bracket Function".

\[
[7.2] = 7
\]

For \( x = 5/2 = 2.5 \) \( \in \mathbb{R}^{+} \),

\[
[5/2] = [2.5] = 2
\]

Similarly, \( [5] = 5 \),

\[
[-3] = -3, \quad [9/2] = [4.5] = -5
\]

Is \( 182 \) a quadratic residue or non-quadratic residue?

\[
182 = -89 \text{ (mod 271)}
\]

\[
q = -89 \text{ (mod 271)} \quad \Rightarrow \quad \frac{-89}{271} = -\frac{89}{271}
\]

\[
271 - 1 = 2 \quad \Rightarrow \quad \left( \frac{89}{271} \right) = \left( \frac{-1}{271} \right) = 1
\]

\[
\left( \frac{89}{271} \right) \left( \frac{271}{89} \right) = \frac{89 - 1 \cdot 271 - 1}{2} = \frac{89 - 1 \cdot 271 - 1}{2} = (-1)^{\frac{44 \cdot 133}{2}} = (-1)^{5946} = 1
\]
\( \left( \frac{189}{271} \right) \) and \( \left( \frac{271}{89} \right) \) has same quadratic character.

\[
\left( \frac{271}{89} \right) = \left( \frac{4}{89} \right)
\]

\[ r \equiv -85 \pmod{89}, \]

\[
\frac{-85}{89} = (-1 \times 5 \times 17)
\]

\[ = (-1) \left( \frac{5}{89} \right) \left( \frac{17}{89} \right) = (-1)^2 \]

\[ = (-1) \left( \frac{5}{89} \right) \left( \frac{17}{89} \right) = (-1) \left( \frac{5 \cdot 17}{89} \right) = (-1) \left( \frac{85}{89} \right) = (-1)^2 \]

Both \( \left( \frac{5}{89} \right) \) and \( \left( \frac{89}{5} \right) \) has same quadratic character.

\[ \left( \frac{89}{271} \right) = 1 \]

\[ eq. (1) \Rightarrow \left( \frac{182}{271} \right) = (-1) \cdot (-1) = 1 \]

Hence 182 is quadratic non-residue of 271.
Prove That

i) \( x = \lfloor x \rfloor + \theta \), \( 0 \leq \theta < 1 \).

ii) \( [x + n] = [x] + n \), \( x \in \mathbb{R} \) and \( n \in \mathbb{N} \).

iii) If \( x, y \in \mathbb{R} \) and \( y > 0 \) then

\[
\lfloor x \rfloor = \frac{x}{y} + \theta \quad \text{where} \quad 0 \leq \theta < y.
\]

iv) \[
\lfloor \frac{x}{n} \rfloor = \left\lfloor \frac{x}{n} \right\rfloor
\]

Proof:

I) This is obviously true by definition.

\[
x = \lfloor x \rfloor + \theta \quad 0 \leq \theta < 1
\]

II \[
[x + n] = [x] + n
\]

Since \( x = \lfloor x \rfloor + \theta \) and \( 0 \leq \theta < 1 \),

\[
[x] = x - \theta
\]

\[
[x] + n = x + n - \theta
\]

\[
\therefore [x] + n = [x + n] + \theta \quad \text{where} \quad \theta \geq 0
\]

as \( [x] \), \( n \) and \( [x + n] \) are
integer so \( \theta_1 - \theta \) must be an integer but \( 0 \leq \theta_1 - \theta < 1 \).

\[ \Rightarrow \theta_1 - \theta = 0 \]

\[ \Rightarrow [x] + n = [x + n] + 0 \]

\[ \Rightarrow [n] + n = [x + n] \]

III

If \( x, y \in \mathbb{R} \) and \( x = qy + \varphi \), \( 0 \leq \varphi < y \)

Then \( [\frac{x}{y}] = q \):

Since \( x = qy + \varphi \)

\[ \frac{x}{y} = q + \frac{\varphi}{y} \]

\[ [\frac{x}{y}] = [q + \frac{\varphi}{y}] \]

\[ = [\frac{x}{y}] + q \quad \text{for} \quad 0 \leq \varphi < y \]

\[ \Rightarrow 0 \leq \frac{\varphi}{y} < 1 \]

\[ [\frac{x}{y}] = q + 0 \]

\[ [\frac{x}{y}] = q \]

So

\[ [\frac{x}{y}] = q. \]
\[ \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor \]

**Proof:**
\[ \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor \]

Since \( [x] \in \mathbb{Z} \) so \( \exists y \) and \( n \) such that
\[ [x] = qn + r \text{ where } 0 \leq r < n \]
\[ \Rightarrow 0 \leq y/n < 1 \]
\[ [x] = q + \frac{y}{n} \quad ; \quad [x] = x - \theta \]
\[ \text{using in eqn 1} \]
\[ x-\theta = qn + \gamma \]
\[ x = qn + \theta + \gamma \]
\[ \frac{x}{n} = \frac{qn + \theta + \gamma}{n} \]
\[ \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{q + \frac{\theta + \gamma}{n}}{n} \right\rfloor \]
\[ = q + \left\lfloor \frac{\theta + \gamma}{n} \right\rfloor \]
\[ \left\lfloor \frac{x}{n} \right\rfloor = q + \theta \]
\[ \left\lfloor \frac{x}{n} \right\rfloor = q - \theta \]

Since \( [x] = qn + \gamma \); \( 0 \leq \gamma < n \)
\[
\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{y + \frac{2}{n}}{n} \right\rfloor = \left\lfloor \frac{y}{n} + \frac{2}{n^2} \right\rfloor = y + \left\lfloor \frac{2}{n^2} \right\rfloor \\
= y + 0 = y \quad : \quad \left\lfloor \frac{x}{n} \right\rfloor = 0 \quad \quad 0 \leq \left\lfloor \frac{y}{n} \right\rfloor < 1
\]

\( \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor = y \rightarrow (3) \)

From (2) & (3) we get

\[
\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x}{y} \right\rfloor
\]

Theorem:

\[
\left\lfloor \frac{x/y}{y} \right\rfloor = \left\lfloor \frac{x}{y^2} \right\rfloor
\]
An even integer is perfect.

\[ \sigma(n) = \sigma_1(n) = \sum_{d|n} d \]

Theorem: If \( n = \prod_{i=1}^{r} p_i^{a_i} \) where \( p_i \) are distinct primes

\[ d(n) = \prod_{i=1}^{r} (a_i + 1) \]

\[ \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1} \]

A number \( n \geq 2 \) is perfect if \( \sigma(n) = 2n \).

All perfect numbers are even.
A function $f$ is said to be arithmetic if its domain is the set of integer. A single valued arithmetic function is called regular or multiplicative if $f(mn) = f(m)f(n)$.

Def: $d(n) = \tau(n)$ the number of the divisor of $n$.

$\tau(8) = 4$.

$S(n) =$ the sum of the divisor of $n$.

$S(8) = 1 + 2 + 4 + 8 = 15$.

Furthemore, the function $d(n) = \tau(n)$ and $S(n)$ are multiplicative.

$\tau(mn) = \tau(m) \tau(n)$.

$S(mn) = S(m) S(n)$, such that

$\forall (m, n) = 1$. 
Let \( n = p_1^{d_1} p_2^{d_2} \ldots \) be the standard form of \( n \). Then

\[
\begin{align*}
\text{i) } \quad d(n) &= \pi(\pi'(n)) = \prod_{i=1}^{\ell} (a_i + 1), \\
\text{ii) } \quad S(n) &= \prod_{i=1}^{\ell} \frac{p_i^k - 1}{p_i - 1}
\end{align*}
\]

**Proof:** The divisors of \( p_1^{d_1} \)

1. \( p_1^1, p_1^2, \ldots, p_1^{d_1} \)

\[
\tau(p_1^{d_1}) = d_1 + 1
\]

\[
\tau(p_1^{d_1}) \cdot \tau(p_2^{d_2}) \cdot \tau(p_3^{d_3}) \ldots \tau(p_{\ell}^{d_{\ell}})
\]

\[
\Rightarrow \quad \tau(n) = (d_1 + 1)(d_2 + 1) \ldots (d_\ell + 1)
\]

\[
= \prod_{i=1}^{\ell} (a_i + 1)
\]

\[
\text{ii) } \quad \text{Now}
\]

\[
S(n) = S(p_1^{d_1} p_2^{d_2} p_3^{d_3} \ldots p_{\ell}^{d_{\ell}})
\]

\[
= S(p_1^{d_1}) \cdot S(p_2^{d_2}) \cdot S(p_3^{d_3}) \ldots \cdot S(p_{\ell}^{d_{\ell}})
\]

\[
S(p_1^{d_1}) = 1 + p_1^1 + p_1^2 + \ldots + p_1^{d_1} - 1
\]
This is a geometric series

with \( r = \beta \), \( a = 1 \) and \( n = \alpha + 1 \).

\[
S_n = a \left( \frac{r^n - 1}{r - 1} \right)
\]

\[
S_n = \frac{\beta^{\alpha + 1} - 1}{\beta - 1}
\]

Similarly

\[
S(\beta^{\alpha_2}) = \frac{\beta^{\alpha_2 + 1} - 1}{\beta^{\alpha_2} - 1}
\]

\[
S(\beta^{\alpha_3}) = \frac{\beta^{\alpha_3 + 1} - 1}{\beta^{\alpha_3} - 1}
\]

\[
S(\beta^{\alpha_r}) = \frac{\beta^{\alpha_r + 1} - 1}{\beta^{\alpha_r} - 1}
\]

So the equation is

\[
S(n) = \frac{\beta^{\alpha_1 + 1} - 1}{\beta^{\alpha_1} - 1} \left( \frac{\beta^{\alpha_2 + 1} - 1}{\beta^{\alpha_2} - 1} \right) \cdots \left( \frac{\beta^{\alpha_r + 1} - 1}{\beta^{\alpha_r} - 1} \right)
\]

\[
S(n) = \prod_{i=1}^{r} \frac{\beta^{\alpha_i + 1} - 1}{\beta^{\alpha_i} - 1}
\]
Möbius function:

Let \( m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k} \)
be the standard form of \( m \)
and \( p_i \) for \( i = 1, 2, 3, \ldots, k \) are
distinct primes. Then we take

\[
\mu(m) = \begin{cases} 
0 & \text{if any } a_i > 1 \\
(-1)^b & \text{if all } a_i = 1 \\
1 & \text{if all } a_i = 0
\end{cases}
\]

To define \( \mu(m) \) is called

Möbius function of \( m \).

E.g.

\[ 24 = 2^3 \cdot 3 \]

\[
\mu(24) = 0 \quad \because \quad 3 > 1
\]

\[
\mu(30) = \begin{cases} 
(-1)^3 & \text{if all } a_i = 1 \\
1 & \text{if all } a_i = 0
\end{cases}
\]

\[ 30 = 2 \cdot 3 \cdot 5 \]

\[ a_1 = 1 \]

\[ \mu(1) = 1 \]

\[ \mu(1) = 1 \]

\[ \mu(1) = 1 \]
\[
\left[ \frac{n}{2} \right] = \left[ \frac{n}{y} \right]
\]

L.H.S

Since \( n = y + z \), \( 0 \leq z < y \).

Dividing both sides by \( y \).

\[
\frac{n}{y} = \frac{y + z}{y}
\]

Taking bracket from both sides.

\[
\left[ \frac{n}{y} \right] = \left[ \frac{y + z}{y} \right]
\]

\[
= \left[ \frac{y}{y} \right] + \left[ \frac{z}{y} \right], \quad \left[ \frac{z}{y} \right] = 0
\]

\[
\left[ \frac{n}{2} \right] = \left[ \frac{y}{2} \right] + 0
\]

\[
\left[ \frac{n}{2} \right] = \frac{y}{2} - 1 \quad \text{(i)} \quad \text{as} \quad y \geq 2.
\]

\[
\left[ \frac{n}{2} \right] = \frac{y}{2} \quad \text{for} \quad y \leq 2.
\]

R.H.S

\[
\left[ \frac{n}{y} \right]
\]

\[
\therefore \quad \frac{n}{y} = y + z; \quad 0 \leq z < y
\]
\[
\frac{x}{y} = \frac{y}{x} + \frac{z}{y}.
\]

\[
\frac{1}{y^2} = \frac{y}{x} + \frac{z}{y^2}.
\]

\[
\left[ \frac{x}{y^2} \right] = \left[ \frac{y}{x} + \frac{z}{y^2} \right]
\]

\[
\left[ \frac{x}{y^2} \right] = \left[ \frac{y}{x} \right] + \left[ \frac{z}{y^2} \right] \quad ; \quad 0 \leq \frac{x}{y^2} < 1.
\]

\[
\left[ \frac{x}{y^2} \right] = \left[ \frac{y}{x} \right] + 0.
\]

\[
\left[ \frac{x}{y^2} \right] = \frac{1}{2} \quad (2) \quad \Rightarrow \quad \left[ \frac{y}{x} \right] = \frac{y}{x}.
\]

Since

From (1) and (2) we see \( y/x \in \mathbb{Z} \).

\[
\left[ \frac{x}{y} \right] = \left[ \frac{y}{x} \right]
\]

\[
\frac{x}{y}
\]