CHANDERNAGORE COLLEGE

CONGRUENCE AND IT'S APPLICATION

NAME: RONAK SARKAR

UNDER SUPERVISION: Dr. AMALENDU GHOSH

DEPARTMENT: MATHEMATICS

COURSE: B.Sc. (HONOURS)

SEMESTER: VI

PAPER CODE: BMH6PW01

COLLEGE ROLL NO.: 21MTMH42

REGISTRATION NO.: 202101050600 OF 2021-22

UNIVERSITY ROLL NO.: 210340400067

CHANDERNAGORE COLLEGE

DEPARTMENT OF MATHEMATICS

(PROJECT COMPLETATION CERTIFICATE)

TO WHOME IT MAY CONCERN

THIS IS TO CERTIFY THAT **RONAK SARKAR** STUDENT OF B.Sc. MATHEMATICS HONOURS SEM VI HAS SUCCESSFULLY COMPLETED HIS PROJECT ON "*CONGRUENCE AND IT'S APPLICATION*" UNDER THE SUPERVISION OF DR. AMALENDU GHOSH ASSOCIATE PROFESSOR, CHANDERNAGORE COLLEGE.

Supervisor
(Dr. Amalendu Ghosh)

ACKNOWLEDGEMENT

I would like to thank Dr. Amalendu Ghosh for his kind help and guidance. I appreciate his patience and willingness to help me throughout this project in the right direction and allowed me to enjoy the success of forming a conclusion of my own. Also, various sources of internet have helped me a lot in doing this project. I would also like to express my sincere thanks all of my teachers at Chandernagore College who have given me such a strong knowledge in mathematics.

____

(Student's signature)

CONTENT.

NOTATIONS:

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of natural integers
$\mathbb{Q}$	Set of natural rational numbers
$\mathbb{R}$	Set of natural real numbers
gcd(a, b)	Greatest common divisor of the integers a and b
lcm(a, b)	Least common multiple of the integers a and b
$f(x)$	Function of x
$t \mid s$	t divides s
$t \nmid s$	t does not divide s
$\in$	Belongs to
$\forall$	For all
$\exists$	There exist

❖ Introduction

Another approach to divisibility questions is through the arithmetic of remainders or the theory of congruence. The concept of congruence was first introduced by German mathematician **Karl Friedrich Gauss** (1777-1855) in his **Disquisition of Arithmeticae**.

The method of getting sum of n consecutive natural numbers was confessed by him that is,

$$\begin{array}{cccccc} 1 & 2 & 3 & \dots\dots & n-1 & n \\ n & n-1 & n-2 & \dots\dots & 2 & 1 \end{array}$$

Adding all n vertical columns, we get n numbers which all are equal to $(n+1)$ and adding these n terms we get $n(n+1)$. This shows two times sum of n consecutive natural numbers are $n(n+1)$.

Therefore, the sum of n consecutive natural numbers is

$$\frac{n(n+1)}{2}$$

❖ CONGRUENCE

▪ DEFINITION

Let m be a fixed positive integer. Two integers a and b are said to be $congruent\ modulo\ m$ if $(a - b)$ is divisible by m that is $(a - b) = km$. Symbolically it is expressed as $a \equiv b\ (mod\ m)$.
Example, let take $m = 5$. Then $16\ \equiv 1\ (mod\ 5)$.
If we take $m = 19$. Then $60 \equiv 3\ (mod\ 19)$.
When $(a - b)$ is not divisible m, a is said to be incongruent b modulo m. It is expressed as $a \not\equiv b\ (mod\ m)$
Example, $6\ \not\equiv 1\ (mod\ 2)$.

Note. When $m = 1$ then every two integers are congruent to modulo m.

▪ PROPERTES OF CONGRUENCE

1. $\boldsymbol{a\ \equiv\ a\ (mod\ m)}$.

Proof. We know $(a - a) = 0, \forall a \in \mathbb{Z}$.
For all positive integers m, we get $m|0$.
or, $m|(a - a)$.
Therefore, $a \equiv a\ (mod\ m)\ \forall\ a \in \mathbb{Z}$ and $m \in \mathbb{N}$.

2. If $\boldsymbol{a \equiv b\ (mod\ m)}$ then $\boldsymbol{b \equiv a\ (mod\ m)}$.

Proof. We have $a \equiv b\ (mod\ m)\ \forall\ a, b \in \mathbb{Z}$ and $m\ \in\ \mathbb{N}$.
Therefore, $m\ |\ (a - b)$.
Or, $\frac{(a - b)}{m} = k$, for some integer k.
Or, $\frac{-(b - a)}{m} = k$
Or, $\frac{(b - a)}{m} = -k$, $-k$ is also an integer.
Therefore, $b \equiv a\ (mod\ m)\ \forall\ a, b\ \in\ \mathbb{Z}$ and $m \in \mathbb{N}$.

3. If $\boldsymbol{a \equiv b\ (mod\ m)}$ and $\boldsymbol{b \equiv c\ (mod\ m)}$ then $\boldsymbol{a \equiv c\ (mod\ m)}$.

Proof. We have, $a \equiv b\ (mod\ m)$ …… (1)
and $b \equiv c\ (mod\ m)$…… (2) $\forall\ a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$.
From (1) and (2) we can write $(a– b) = ms$ …… (3)
And $(b - c) = mr$ …… (4) for some integers s and r.
From equation (4) we get $b = mr + c$.
Putting this value of b in equation (3) we get
$\{a– (m.r + c)\} = ms$
$Or, (a– mr– c) = m.s$

$Or, (a - c) = ms + mr$

$Or, (a– c) = m(r + s), (r + s)$ is also an integer.

$Or, a \equiv c \ (mod\ m)$.

Therefore, , $a \equiv c \ (mod\ m)\ \forall\ a, c \in \mathbb{Z}$ and $m \in \mathbb{N}$.

4. If $\boldsymbol{a \equiv b \ (mod\ m)}$ then for any integer $\boldsymbol{c}$

i. $\boldsymbol{(a + c) \equiv (b + c)(mod\ m)}$.

Proof. We have $a \equiv b \ (mod\ m)\ \forall\ a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$.

Then $(a– b) = km$, for some integer k.

$Or, a + c– c – b = km$

$Or, (a + c)– (c + b) = km$

Therefore, $(a + c) \equiv (c + b)(mod\ m) \forall\ a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$.

ii. $\boldsymbol{(a.c) \equiv (b.c)(mod\ m)}$.

*Proof***.** We have $a \equiv b \ (mod\ m)\ \forall\ a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$.

Then $(a– b) = km$, for some integer k.

Or, $c(a– b) = c.km,\ c \in \mathbb{Z}.$

$Or, c.a - c.b = (c.k)m, (c.k) \in \mathbb{Z}$

Therefore, $(a.c) \equiv (b.c)(mod\ m), \forall\ a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$.

5. If $\boldsymbol{a \equiv b \ (mod\ m)}$ and $\boldsymbol{c \equiv d \ (mod\ m)}$then

i. $\boldsymbol{(a + c) \equiv (b + d)(mod\ m)}$

*Proof***.** $a \equiv b \ (mod\ m)$ …… (1)

and $c \equiv d \ (mod\ m)$ …… (2) $\forall\ a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

From (1) and (2) we can write $(a - b) = m.s$ …… (3)

And $(c - d) = m.r$…… (4) for some integers s and r.

Adding equation (3) and (4) we get

$a - b + c - d = m.s + m.r$

$Or, (a + c) - (b + d) = m(s + r)$

Therefore, $(a + c) \equiv (b + d)(mod\ m) \forall\ a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

ii. $\boldsymbol{(a.c) \equiv (b.d)(mod\ m)}$

Proof. We have, $a \equiv b \ (mod\ m)$ …… (1)

and $c \equiv d \ (mod\ m)$ …… (2) $\forall\ a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

Now by property 4 we can write from (1),

$a.c \equiv b.c \ (mod\ m)$…… (3)

And from (2), $b.c \equiv b.d \ (mod\ m)$…… (4)

Again, by property (3) from (3) and (4) we can write

$a.c \equiv b.d \ (mod\ m)$.

Therefore, $a.c \equiv b.d \ (mod\ m) \forall\ a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

6. **If $\boldsymbol{a \equiv b \ (mod\ m)}$ and $\boldsymbol{d|m, d > 0}$ then $\boldsymbol{a \equiv b \ (mod\ d)}$**

Proof. We have$d|m\ so\ m = k.d$, for some integer k.
Now, $a \equiv b\ (mod\ m)$
$Or, a - b = l.m,$ for some integer l.
$Or, a - b = lkd$
$Or, a - b = (l.k)d$
Therefore, $a \equiv b\ (mod\ m)$.

- **RESIDUE**

If $a \equiv b\ (mod\ m)$ then b is said to be the *residue* of a modulo m and if $0 \leq b \leq m - 1$ then b is called the *least non-negative residue of a modulo m.*

Theorem 1. For any two integers $\boldsymbol{a}$ and $\boldsymbol{b}$, $\boldsymbol{a \equiv b\ (mod\ m)}$ if and only if $\boldsymbol{a}$ and $\boldsymbol{b}$ leave same remainder when divided by $\boldsymbol{m}$.

*Proof***.** Let r be the remainder when a is divided by m. then there exists an integer q such that $a = q.m + r, 0 \leq r \leq m - 1$.
Since $a \equiv b\ (mod\ m)$ so $a - b = k.m$ where k is an integer.
Therefore, $b = a - k.m$
$Or, b = q.m + r - k.m$
$Or, b = (q - k)m + r$
This shows that b leaves same remainder r.
Conversely, let r be the remainder a and b are divided by m. Then there exist two integers p and q such that
$a = p.m + r, b = q.m + r$
Therefore, $a - b = p.m + r - q.m - r$.
$Or, a - b = (p - q)m, i.e., m \mid (a - b)$
This proves that $a \equiv b\ (mod\ m)$.

Theorem 2. If $\boldsymbol{a \equiv b\ (mod\ m)}$ then $\boldsymbol{a^n \equiv b^n}$ $(\mathbf{mod\ m})$for all positive integers $\boldsymbol{n}$.

Proof. We use the principal of induction to prove the theorem.
The theorem is true for $n = 1$. Let us assume the theorem is true for $n = k$. then $a^k \equiv b^k\ (mod\ m)$.
Now $a \equiv b\ (mod\ m)$ and $a^k \equiv b^k\ (mod\ m)$ together imply that
$a^{k+1} \equiv b^{k+1}\ (mod\ m)$
This shows that the theorem is true for $k + 1$ if the theorem for every positive integer k.
By the principal of induction, the theorem is true for every positive integer n.

Note. Converse of this theorem does not necessarily hold. That is $a^k \equiv b^k\ (mod\ m)$ does always imply $a \equiv b\ (mod\ m)$.
For example, $5^2 \equiv 2^2$ (mod 7) but $5 \not\equiv 2$ (mod 7).

Theorem 3. If $d = \mathrm{gc\,d}(x,m)$then $xa \equiv xb\ (mod\ m) \Leftrightarrow a \equiv\ b\ (mod\ \frac{m}{d})$.

Proof. We have $d = gcd(x,m)$ then there exist two integers r, s which are relatively prime such that $x\ =\ dr$ and $m\ =\ ds$.
$xa - xb\ =\ qm$ where q is an integer.
Therefore, $dra - drb\ =\ qds$
$Or, a - b = \frac{\mathrm{qs}}{\mathrm{r}}$.
Since $a - b$ is an integer then $r\ |qs. r$ and s are relatively prime so $r|\ q,$ say that is k.
Therefore, $a– b = ks$
$Or, a - b\ =\ \frac{km}{\mathrm{d}}$
$Or, a\ \equiv\ b\ \left(mod\ \frac{m}{d}\right)$.
Conversely. $a \equiv b(mod\ \frac{m}{d})$ imply $\frac{m}{d}\ |\ (a - b)$
$Or, m\ |\ d(a - b)$
$Or, m\ |\ x(a - b)$
Therefore, $xa\ \equiv\ xb\ (mod\ m)$.

Corollary 1. When $gcd(x,m) = 1$ then $xa \equiv xb(mod\ m) \Leftrightarrow a \equiv b(mod\ m)$.

Corollary 2. When $gcd(x,m) = x$ then $xa \equiv xb(mod\ m) \Leftrightarrow a \equiv\ b(mod\ \frac{m}{x})$.

- ## Worked examples

1. Find the least positive residue in 4^{30}(mod 11).

we know $4^2 \equiv 5$ (mod11)
Or, $4^{30} \equiv 5^{15}$ (mod 11) …… (i)
Now, $5^2 \equiv 3$(mod 11)
Or, $5^{14} \equiv 3^7$(mod 11)
Or, $5^{15} \equiv (-6)3^7$ (mod 11)
Or, $5^{15} \equiv (-2)3^8$ (mod 11) ……(ii)
Again, $3^3 \equiv 5$(mod 11)
Or, $3^6 \equiv 5^2$ (mod 11)
Or, $3^6 \equiv 3$ (mod 11)
Or, $3^5 \equiv 1$ (mod 11)
Or, $3^8 \equiv 5$ (mod 11)
Or, $(-2)3^8 \equiv -10$ (mod 11)
Or, $(-2)3^8 \equiv 1$ (mod 11)

Hence, from (i) and (ii)
$4^{30} \equiv 1$ (mod 11).
Therefore, the least positive residue of 4^{30}(mod 11) is 1.

2. **Use the theory of congruence to establish $\mathbf{73|(2^{36}-1)}$.**

We know $2^6 \equiv (-9)(mod\ 73)$
$or, 2^{12} \equiv 81(mod\ 73)$
$or, 2^{12} \equiv 8(mod\ 73)$
$or, 2^{24} \equiv 64(mod\ 73)$
$or, 2^{24} \equiv (-9)(mod\ 73)$
$or, 2^{36} \equiv (-72)(mod\ 73)$
$or, 2^{36} \equiv 1(mod\ 73)$
Therefore 73 divides $(2^{36}-1)$.

3. **Find the remainder when $\sum_{k=1}^{100}(\mathbf{k}!)$ divided by 10.**

We know 5! ≡ 0 (mod 10)
That is for all n> 5, n! ≡ 5!.6.7.8…n.
Then n! ≡ 0.6.7…n (mod 10), ∀ n >5.
Then $\sum_{k\equiv 5}^{100}(\mathrm{k}!)$ ≡ 0 (mod 10).
So, we have to find (1 + 2! + 3! + 4!) (mod 10).
(1 + 2! + 3! + 4!) ≡ 33
And 33≡ 3 (mod 10)
Hence, $\sum_{k\equiv 1}^{100}(\mathrm{k}!)$ ≡ 3 (mod 10).

4. **Use congruence to prove $\mathbf{7|(2^{5n+3}+5^{2n+3})}$ for all $\boldsymbol{n} \geq \mathbf{1}$.**

$2^{5n+3}+5^{2n+3} = 8.32^n + 125.25^n$
$32^n - 25^n = 0$ (mod 7) for all n ≥ 1.
Therefore, $8.32^n - 8.25^n = 0$ (mod 7) for all n ≥ 1.
Also, we have $133(25)^n = 0$ (mod 7) for all n ≥ 1.
Therefore $8.32^n + 125.25^n = 0$ (mod 7) for all n ≥ 1.
This implies 7 | $2^{5n+3} + 5^{2n+3}$ for all n ≥ 1.

- **DIVISIBILITY TEST.**

This is an interesting applications of congruence theory, involves finding special criteria under which a given integer is divisible by another integer. These divisibility tests depend on the system used to assign integers. Particularly, we use 10 as the base for our number system. This can also be shown for different base of number system as 8 (Octal system), 16(Hexadecimal system).

First, we will start by showing for any given integer b>1, a positive number N can be expressed uniquely in the term of power of b.

For any integer b>1, a positive number N is divided by b then by division algorithm there exist two integers q_1 and a_0 such that,

$\mathrm{N} = q_1 b + a_0 \ldots\ldots$(i) $0 \le a_0 < \mathrm{b}$.

If q_1>b then again by division algorithm their exist two integers q_2 and a_1 such that

$q_1 = q_2 b + a_1 \quad 0 \le a_1 < \mathrm{b}$.

Substituting the value of q_1 in equation (i) we get

N = $(q_2 \mathrm{b} + a_1)\mathrm{b} + a_0$

Or, $N = q_2 b^2 + a_1 b + a_0 \ldots\ldots$(ii)

As long as $q_i \ge$ b, we will continue the same process. Going one more step:

$N = q_3 b^3 + q_2 b^2 + a_1 b + a_0 \ldots\ldots$(iii)

At nth stage, where $q_{n-1} = q_n b + a_{n-1}$, $0 \le a_{n-1} < \mathrm{b}$.

And $0 \le q_n \le b$. Setting $a_n = q_n$, we reach the representation

$N = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$.

This expression was our aim.

To show the uniqueness of this expression, if possible, let N has two distinct representations; say,

$N = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$

$N = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0$.

With $0 \le a_i < \mathrm{b}$ and $0 \le c_i < \mathrm{b}$ for each i. Subtracting the second representation from first gives the equation

$0 = d_n b^n + d_{n-1} b^{n-1} + \cdots + d_1 b + d_0$,

Where $d_i = a_i - c_i$, $i = 1, 2, \ldots, n$. As two representations are assumed different, we must have $d_i \ne 0$ for some value of i. Take k to be the smallest subscript for which $d_k \ne 0$. Then

$0 = d_n b^n + d_{n-1} b^{n-1} + \cdots + d_k b^k$.

Dividing this by b^k, $0 = d_n b^{n-k} + d_{n-1} b^{n-k-1} + \cdots + d_k$

$or, -d_k = d_n b^{n-k} + d_{n-1} b^{n-k-1} + \cdots + d_{k+1} b$

$or, -d_k = b(d_n b^{n-k-1} + d_{n-1} b^{n-k-2} + \cdots + d_{k+1})$

This tells us that $b \mid d_k$. Now the inequalities $0 \le a_k < \mathrm{b}$ and $0 \le c_k < \mathrm{b}$ lead to $-\mathrm{b} < a_k - c_k < \mathrm{b}$, $or\ |d_k| < b$. The only possible thing is that $d_k = 0$. Which is impossible. From this contradiction we can say N has only one unique expression.

Some unique representations of decimal numbers.

Let us take a decimal number 2759.

The unique representation of the number in the terms of power of 10 is

2759 = $2 * 10^3 + 7 * 10^2 + 5 * 10 + 9$.

This is called decimal expression.

We can write 2759 in the terms of power of 8 as

$2759 = 5 * 8^3 + 3 * 8^2 + 0 * 8 + 7$

Hence the octal representation of $(2759)_{10}$ is $(5307)_8$

We can write 2759 in the terms of power of 2 as

$$2759 = 1 * \ 2^{11} + 0 * 2^{10} + 1 * 2^9 + 0 * 2^8 + 1 * 2^7 + 1 * 2^6$$
$$+0 * 2^5 + 0 * 2^4 + 0 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1$$

The binary representation of $(2759)_{10}$ is $(101011000111)_2$

Theorem 4. **Let $\boldsymbol{f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0}$ where $\boldsymbol{a_k \in \mathbb{Z}, \mathrm{k} = 0, 1, \ldots, \mathrm{n}}$, if $\boldsymbol{a \equiv b \ (mod\ m)}$. Then $\boldsymbol{f(a) \equiv f(b)(mod\ m)}$.**

Proof. We know if $a \ \equiv b \ (mod\ m)$ then $a^k \equiv b^k \ (mod\ m), \forall k > 1.$

and $a_k a^k \equiv a_k b^k \ (mod\ m), \forall \ k \geq 0$

Adding all such relations for $k = 0,1, \ldots, n$. We get

$\sum_{k=0}^{n} a_k a^k \equiv \ (\sum_{k=0}^{n} a_k b^k \ )(mod \ \ m)$

$or, \ f(a) \equiv f(b)(mod\ m).$

Theorem 5. **Condition for a positive decimal number to be divisible by 9.**

Proof. Our key observation is $10 \equiv 1 \ (mod\ 9)$.

Now the number N can be uniquely expressed in the terms of power of 10.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integral coefficient.

Then $N = f(10) = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ and

$f(1) = a_n + a_{n-1} + \cdots + a_1 + a_0 = t \ (say)$

Hence by theorem 4, $f(10) \equiv f(1)(mod\ 9)$ so that $N \equiv t(mod\ 9)$.

It follows that $N \equiv 0 \ (mod\ 9)$ if and only if $t \equiv 0(mod\ 9)$.

Conclusion: N, a positive decimal number is divisible by 9 if and only if the sum of the digits of the number is divisible by 9.

Theorem 6. Condition for a positive decimal number to be divisible by 11.

Proof. Our key observation is $10 \equiv (-1) \ (mod\ 11)$.

Now the number N can be uniquely expressed in the terms of power of 10.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integral coefficient.

Then $N = f(10) = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ and

$f(-1) = a_0 - a_1 + \cdots \ (-1)^n a_n = t \ (say)$

Hence by theorem 4, $f(10) \equiv f(-1)(mod\ 11)$ so that $N \equiv t(mod\ 9)$.

It follows that $N \equiv 0 \ (mod\ 11)$ if and only if $t \equiv 0(mod\ 11)$.

Conclusion: N, a positive decimal number is divisible by 11 if and only if the difference of the sum of the digits at odd places and even places of the number is divisible by 11.

Another method of expression is in the terms of power of
(1000).
Let M = $a_n 1000^n + a_{n-1}1000^{n-1} + \cdots + a_1 1000 + a_0$. Where a_k is integer, $0 \leq a_k \leq 999, k = 0,1, \ldots, n$.
We know $1001 \ = \ 7 * 11 * 13$ and $999 = 27 * 37$
Therefore, $1000 \equiv (-1) \ (mod \ 7)$
Or, $1000 \equiv (-1) \ (mod \ 13)$
And $1000 \equiv (1) \ (mod \ 37)$
Or, $1000 \equiv (1) \ (mod \ 27)$
From the previous conclusions we can say,

1. A positive decimal number, M is divisible by 7 if and only if difference of the sum of the digits at odd places and even places of the number is divisible by 7.

2. A positive decimal number, M is divisible by 13 if and only if difference of the sum of the digits at odd places and even places of the number is divisible by 13.

3. A positive decimal number, M is divisible by 27 if and only if the sum of the digits of the number is divisible by 27.

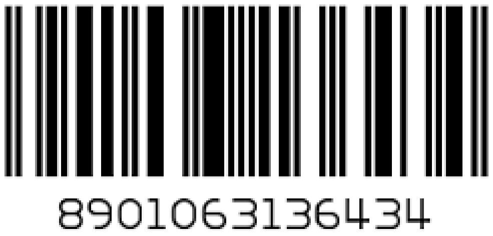
4. A positive decimal number, M is divisible by 37 if and only if the sum of the digits of the number is divisible by 37.

For example, let us take the number 35078571.
The sum of the digits of the number are $3 + 5 + 0 + 7 + 8 + 5 + 7 + 1 = 36$, which is divisible by 9.
Hence 35078571 is divisible by 9.
Again $3 - 5 + 0 - 7 + 8 - 5 + 7 - 1 = 0$,which is divisible by 11.
Hence 35078571 is divisible by 11.

Let take another number 23146512.
$23146512 = 23(1000)^2 + 146(1000) + 123$.
23146512 is divisible by 7 because $123 - 146 + 23 = 0$ which is divisible by 7.
The same argument proves 23146512 also divisible by 13 and 11.

Check digit

In our everyday life we find many consumer goods in packets with some identification number consist of some numbers. I am giving some pictures of them in support of the statement.



ISBN

We first describe how congruences are used to detect errors in strings of digits which are used to identify books.

Since 1972 all books published throughout the world began to receive coded ten-digit numerical labels called International Standard Book Numbers (**ISBN**).

For example, the ISBN of the text Abstract Algebra by Herstein is 0-02-353820-1, the ISBN of Discrete Mathematics by Richard Johnsonbaugh (Third edition) is 0-02-360721-1, the ISBN of Discrete Mathematical structures by Kolman, Busby and Ross is 81-203-1147-7. One may see the ISBN of a book on the back of the last cover page or in the beginning of the book.

Now in the ISBN 0-02-353820-1 of Herstein's Abstract Algebra, the leading digit 0 means that the book is published in the English-speaking world like United Kingdom, United States, Australia, Canada. The next group of digits, 02, identifies the publisher (in this case, Macmillan Publishing Company). The third block 353820 is the number assigned to the book by the publisher, that is, 353820 designates this particular book among all those published by Macmillan. The final block of the above ISBN is 1. This number is called the check digit. This check digit makes the ISBN into an example of error-correcting code. With the help of this check digit publishers, book sellers are often able to detect an incorrect ISBN that may occur when the ISBN is incorrectly typed or transmitted by telephone line, or by e-mail etc. and can avoid costly shipping charges that would result from filling an incorrect order.

Formally we describe an ISBN in the following way:

An ISBN is an expression $x_1x_2x_3x_4\,x_5x_6x_7x_8x_9x_{10}$ of ten digits, divided into four blocks; the first block represents the country from where it has been published, the second block represents the publishing company, the third block is the number assigned to the book by the publisher, the final block consists called the check digit. For $i = 1,2, \dots ,9$ each x_i is one of the digits 0,1, 2, …,9. The check digit x_{10} has eleven possible values: 0,1,2,3,4,5,6,7,8,9,10. Notice that if x_{10} is 10 then this check digit consists of two digits. Since we use only one digit to represent the check digit, we replace digit consists of two digits. Since we use only one digit to represent the check digit, we replace 10 by X. Thus, the possible check digits for an ISBN are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X.

We now explain how a check digit is assigned to a particular book. For this we take the help of congruence. Suppose the first nine digits $x_1x_2x_3x_4\, x_5x_6x_7x_8x_9$ of an ISBN are chosen. Then the check digit x_{10} which is one of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X is determined by the congruence

$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} \equiv (mod\ 11).$
That is, $\sum_{i=1}^{9} ix_i + 11x_{10} - x_{10} \equiv 0(mod\ 11)$
$or, \sum_{i=1}^{9} ix_i \equiv x_{10}(mod\ 11)$

Example: Let first 9 digit of the ISBN of a particular book be 0-673-38582. Then the check digit x_{10} is given by

$1.0 + 2.6 + 3.7 + 4.3 + 5.3 + 6.8 + 7.5 + 8.8 + 9.2 \equiv x_{10}(mod\ 11).$
That is,
$12 + 21 + 12 + 15 + 48 + 35 + 64 + 18 \equiv x_{10}(mod\ 11).$
$225 \equiv x_{10}(mod\ 11)$
Hence, $x_{10} = 5.$

We now explain why this ISBN has been created. Now days, many publishers computerize their inventories and billing procedures. A serial number of standardized length and format is far easier to handle by computer than the alternative identification by title, author, edition, etc. Orders received by ISBN can be processed easily than the orders received by title, author, edition, etc. The ISBN system saves much time and labour, because the cumbersome title and author look-up can be avoided. With the help of ISBN, we can also overcome language barriers. An Indian buyer can place an order by telephone to a Japanese publisher without specifying the book's Japanese title. The ISBN system serves the needs of all parties in the book distribution system. For example, confusion about sets of books vs., their individual volumes is avoided the set receives one ISBN and each volume receives its own. Different editions of the same title receive different ISBN's.

Detection of single error in ISBN

It is natural that errors may occur as people enter numerical data into a computer or typewriter. Also, transmission over telephone or microwave channels can lead to errors. We show that a single error can be detected by using the check digit. Let $x_1x_2x_3x_4\,x_5x_6x_7x_8x_9x_{10}$ be a correct ISBN for a book. During billing procedure, suppose a single error has been made in the $\imath$th place, instead of x_i, y_i has been printed, where $x_i \neq y_i$.

For example, the correct ISBN of a particular book is 0-673-38582-5. During billing procedure, suppose it has been printed as 0-678-38582-5 That is, in the 4th place instead of 3, 8 has been printed. This is a single error. We now show that this kind of single error can be detected.

Since $x_1x_2x_3x_4\,x_5x_6x_7x_8x_9x_{10}$ is a correct ISBN, we find that
$\sum_{i=1}^{10} ix_i \ \equiv 0(mod\ 11)$

Now the changed ISBN is $y_1y_2y_3y_4\,y_5y_6y_7y_8y_9y_{10}$ where $x_k = y_k$for all $k \neq i$ and where $x_i \neq y_i$. Suppose where $x_i > y_i$. Since $0 \leq x_i, y_i \leq 10,$ there exist an integer a such that $x_i = \ y_i + a$ where $a \leq 0 \leq 10$.

Now,

$$y_1 + 2y_2 + 3y_3 + 4y_4 \ + 5y_5 + 6y_6 + 7y_7 + 8y_8 + 9y_9 + 10y_{10}$$
$$= x_1 + 2x_2 + 3x_3 + \cdots + (i-1)x_{i-1} \ + iy_i + (i+1)x_{(i+1)} + \cdots$$
$$+9x_9 + 10x_{10}$$
$$= x_1 + 2x_2 + 3x_3 + \cdots + (i-1)x_{(i-1)} + ix_i + i(-a)$$
$$+(i+1)x_{(i+1)} + \cdots + 9x_9 + 10x_{10}$$
$$= \sum_{i=1}^{10} ix_i \ + i(-a)$$
$$\equiv \big(0 + i(-a)\big)\ (mod\ 11)$$

Thus, $\sum_{i=1}^{10} iy_i \ \equiv i(-a)(mod\ 11)$

If $y_1y_2y_3 \ldots y_9y_{10}$ is a correct ISBN, then $\sum_{i=1}^{10} iy_i \ \equiv 0(mod\ 11)$

In that case

$0 \equiv i(-a)(mod\ 11)$

$or, ia \equiv 0(mod\ 11)$

Hence 11 divides ia. Since 11 is a prime number, it follows that either 11 divides a or 11 divides i. But $1 \leq i \leq 10$, $0 \leq a \leq 10$.

Hence 11 cannot divide ia. Thus, we conclude that $y_1y_2y_3y_4\,y_5y_6y_7y_8y_9y_{10}$ is not a valid ISBN.

If $x_i < y_i$ proceeding as above we can prove that $y_1y_2y_3y_4\,y_5y_6y_7y_8y_9y_{10}$ is not a correct ISBN.

Detection error in an ISBN due to interchange of two unequal digits.

We consider the error of the form $x_1x_2x_3x_4\,x_5x_6x_7x_8x_9x_{10} \to$ $x_1x_2 \ldots x_jx_{i+1} \ldots x_ix_{j+1} \ldots x_{10}$, where $x_i \neq x_j$, that is while typing the ISBN two unequal digits have been transposed. We now show that this kind of error can also be detected.

Since we have $x_1x_2 \ldots x_ix_{i+1} \ldots x_jx_{j+1} \ldots x_{10}$, as correct ISBN so,

$1x_1 + 2x_2 \ldots + ix_i + (i+1)x_{i+1} \ldots jx_j + (j+1)x_{j+1} + \cdots + 10x_{10} \equiv 0(mod\ 11)$.

Now the changed ISBN is $y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}$

Where $y_k = x_k$ for $k = 1,2,\ldots,i-1$,

$y_i = x_i$

$y_t = x_t$ for $t = i+1, i+2, \ldots j-1$,

$y_j = x_i$

$y_k = x_k$ for $k = j+1, \ldots, 10$,

Now

$$y_1 + 2y_2 + 3y_3 + 4y_4\ + 5y_5 + 6y_6 + 7y_7 + 8y_8 + 9y_9 + 10y_{10}$$

$$= 1x_1 + 2x_2 \ldots + (i-1)x_{i-1}\ + ix_i + (i+1)x_{i+1} + \cdots + (j-1)x_{j-1} + jx_j + (j+1)x_{j+1} + \cdots 10x_{10} - ix_i + ix_j - jx_j + jx_i$$

$$\equiv 0\ - ix_i + ix_j - jx_j + jx_i\ (mod\ 11)$$

$$\equiv i(x_j - x_i) - j(x_j - x_i)(mod\ 11).$$

Hence

$\sum_{i=1}^{10} iy_i \equiv (i-j)(x_j - x_i)(mod\ 11)$

If $y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}$ is a correct ISBN then $\sum_{i=1}^{10} iy_i \equiv 0(mod\ 11)$

Hence implies $0 \equiv (i-j)(x_j - x_i)(mod\ 11)$

That is 11 divides $(i-j)(x_j - x_i)$

Accordingly, either 11 divides $(i-j)$ or 11 divides $(x_j - x_i)$

Since $1 \le i,j \le 10$. Hence 11 does not divides $(i-j)$

Again $x_i \neq x_j$ and $0 \le x_i, x_j \le 10$. Hence 11 does not divides $(x_j - x_i)$. so we conclude that $y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}$ is not a correct ISBN. Hence an error which is due to interchange of two digits can be detected.

Recall that in an ISBN, the first block of number identifies the language or the country where the book is published. Here are the codes for some of the languages and countries,

0	(English) UK, US, Australia, NZ, Canada.
1	(English) South Africa, Zimbabwe.
2	(French) France, Belgium, Canada, Switzerland.
3	(German) Germany. Austria, Switzerland.
4	Japan
5	USSR
7	China
80	Czechoslovakia
81	India

ISSN

We now say few words about ISSN. The international standard serial number is used to label series publications (magazines, newspapers) is the same way an ISBN labels books. ISSN is an eight digits numerical label. The last digit is check digit. For example, ISSN of the journal “Proceeding of American Mathematical Society” is 0002-9939. Here the last digit 9 is the check digit.

Let us know how to find the check digit of an ISSN whose seven digits are chosen as $x_1x_2x_3x_4\,x_5x_6x_7$. If x_8 is the check digit then x_8 satisfy the congruence

$\sum_{i=1}^{8}(9-i)x_i \equiv 0\ (mod\ 11)$

Here $0 \le x_i \le 9$ for $i = 1,2,\dots,7$ and x_8 is one of 0,1, 2, …,9, X.

For the ISSN 0002-993x_8 we see that

$8.0 + 7.0 + 6.0 + 5.2 + 4.9 + 3.9 + 2.3 + x_8 \equiv 0(mod\ 1\ 1).$

$or, 79 + x_8 \equiv 0(mod\ 1\ 1)$

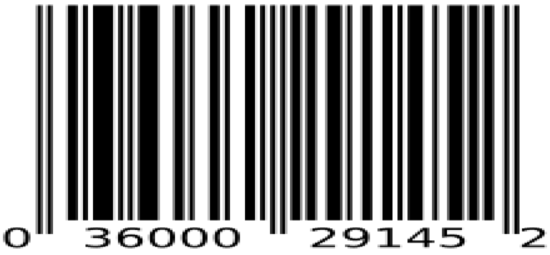
Hence $x_8 = 9$.

Universal Product Code.

Many products are sold in the market have an identification number, Called a universal product number. A universal product code (UPC) is a way to represent a universal product number as a pattern of black and white stripes of various thickness. For this reason, a universal product code is also called a bar code. In many shopping places we see that the cashier at the checkout counter scans the bar code of the item on the scanner and the cash register retrieves the price of the item

There are different versions of UPC. The "UPC-A barcode" is by far the most common and well-known in USA and Canada

A UPC-A consists of 11 digits, (each digit in the range 0 through 9), message data along with a trailing check digit, for a total of 12 digits of barcode data. An example of a typical UPC-A barcode is given in Figure



UPC-A code

The digits of a UPC-A barcode are divided into four blocks.

1. The number system

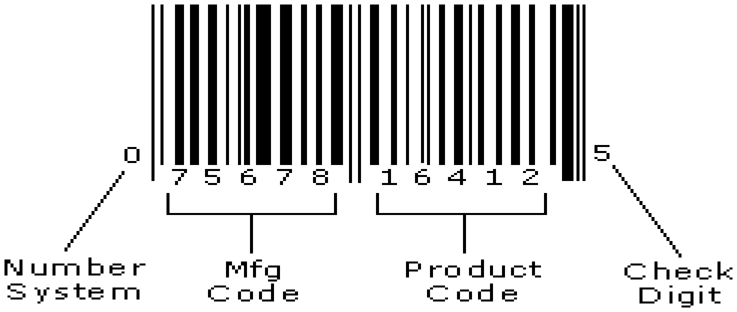
2. The manufacturer code.

3. The product code.

4. The check digit.

The number system digit, usually, is printed just to the left of the bar- code, the check digit just to the right of the barcode, and the manufacturer and product codes are printed just below the barcode, as shown in Figure is in previous page. In the UPC-A the number system is a single digit which identifies the type of the product. The manufacturer code is assigned to the manufacturer by the Universal Code Council (UCC), The product code is assigned to the product by the manufacturer Unlike the manufacturer code, which must be assigned by the Universal Code Council (UCC), the manufacturer is free to assign product codes to each of their products without consulting any other organization.

The International Article Numbering Association EAN assigns the identification numbers to the products manufactured in European countries. This identification number consists of thirteen digits and is known as EAN-13. A typical EAN-13 bar code is shown billow,



An EAN-13 barcode is also divided into four blocks.

1. The number system,

2. The manufacturer code

3. the product code, and

4. the check digit.

Number System: The number system consists of two or three digits which identify the country (or economic region) of the numbering authority which assigns the manufacturer code.

The valid number system codes for some countries are presented here.

00-13: USA and Canada, 30-37: France, 40-44 Germany, 45 Japan (also 49), 471: Taiwan 479: Sri Lanka, 480: 489 Hong Kong, 50: United Kingdom, 880: South Korea, 885. Thailand, 888: Singapore, 890: India, 978: Vietnam, 955: Malaysia, 690-692-China.

Manufacturer Code: The manufacturer code is a unique code assigned to each manufacturer by the numbering authority. All products produced by a given company will use the same manufacturer code.

Product Code: The product code is a unique code assigned by the manufacturer to his product.

Check Digit: The check digit is the last digit used in verifying whether the rest of the data in the barcode has been correctly interpreted. The method of calculating the check digit will be discussed in this section.

Remark: The UCC has announced that from January 1, 2005 all products in USA and Canada must be labelled with EAN-13, a big task for IT professionals. All the 12-digit identification numbers used in USA and Canada are to be replaced by 13-digit identification numbers.

Whether the UPC is of length 12 or 13, we are mainly interested, as in the case of ISBN, in the check digit, which ensures the correctness of the UPC. The methods of determining the check digits for a UPC of length 12 or 13 are the same. However, considering the recent developments, we will focus on UPC of length 13, Le., EAN-13. (We will also indicate how the check digit of UPC strings of length 12 is determined.)

The following string demonstrates a UPC for the Britannia Biscuit Cream Cracker.

8 901063 211070

Here the 13th digit 0 is the check digit. We now explain how this check digit is obtained.

Consider a particular product manufactured by a particular manufacturer.

Then the first 12 digits $x_1x_2x_3x_4\ x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}$ are fixed. The check digit x_{13} is an integer such that $0 \leq x_{13} \leq 10$ and it satisfies the congruence

$$x_{13} \equiv -(1x_1 + 3x_2 + 1x_3 + 3x_4\ + 1x_5 + 3x_6 + 1x_7 + 3x_8 + 1x_9$$
$$+3x_{10} + 1x_{11} + 3x_{12})(mod\ 10)$$

That is

$$1x_1 + 3x_2 + 1x_3 + 3x_4\ + 1x_5 + 3x_6 + 1x_7 + 3x_8 + 1x_9\ \ +3x_{10} + 1x_{11} + 3x_{12} +\ x_{13} \equiv (mod\ 10)$$

Consider the UPC

$$x_{13} \equiv -(1.8 + 3.9 + 1.0 + 3.1 + 1.0 + 3.6 + 1.3 + 3.2 + 1.1 +$$
$$3.1 + 1.0 + 3.7 + 1.0)(mod\ 10)$$

$$x_{13} \equiv -(8 + 27 + 3 + 18 + 3 + 6 + 1 + 3 + 21)(mod\ 10)$$

$x_{13} \equiv -(-2+7+3-2+3-4+1+3+1)(mod\ 10)$
$x_{13} \equiv -10(mod\ 10)$.

$i.e\ x_{13} = 0$

It may be convenient if we use dot product notation to express the above congruence

If $(a_1, a_2, \dots, a_k)$ and $(b_1, b_2, \dots, b_k)$ be two k-tuples, then the dot product of these k-tuples is defined by

$(a_1, a_2, \dots, a_k).(b_1, b_2, \dots, b_k) \equiv 0(mod\ 10)$

With the help of this dot product notation the above congruence can be written as

$(1,3,1,3,1,3,1,31,3,1,3,1).(x_1x_2x_3x_4\ x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13})$

$\equiv 0(mod\ 10)$

For example, the first seven digits of the UPC of Palmolive Shaving Cream is 8901314 and the next five digits 02557. Let us determine the check digit x_{13}. Now this check digit satisfies the congruence

$$(1,3,1,3,1,3,1,3,1,3,1,3,1).(8,9,0,1,3,1,4,0,2,5,5,7,x_{13}) \equiv 0(\text{mod } 10)$$

Then

$$8+27+0+3+3+3+4+0+2+15+5+21+x_{13} \equiv 0$$

$(\text{mod } 10)$.

i.e. $41 + x_{13} \equiv 0(\text{mod } 10)$.

Now $0 \leq x_{13} \leq 10$. Hence the check digit x_{13} is 9. So, we find that the UPC of Palmolive Shaving Cream is 8 901314 025579.

Error Detection in a UPC

We now show that if a single error is made in entering the UPC into a computer, then this error can be detected. Let $x_1x_2x_3x_4\ x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}$ be a UPC. Suppose while typing this number in a computer instead of $x_1x_2x_3x_4\ x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}$, $y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}y_{11}y_{12}y_{13}$ has been typed where $x_k = y_k$ for all $k \neq i$ but $x_i \neq y_i$. Consider this number as a correct UPC. The computer will calculate

(1,3,1,3,1,3,1,3,1,3,1,3,1).$(y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}y_{11}y_{12}y_{13})$ =

$1y_1 + 3y_2 + 1y_3 + 3y_4 + 1y_5 + 3y_6 + 1y_7 + 3y_8 + 1y_9 + 3y_{10} + 1y_{11} + 3y_{12} + 1y_{13}$

Suppose now the i of y_i is odd. Then
(1,3,1,3,1,3,1,3,1,3,1,3,1).$(y_1y_2y_3y_4\ y_5y_6y_7y_8y_9y_{10}y_{11}y_{12}y_{13})$

$= 1y_1 + 3y_2 + 1y_3 + 3y_4 + 1y_5 + 3y_6 + 1y_7 + 3y_8 + 1y_9 + 3y_{10} + 1y_{11} + 3y_{12} +$

$1y_{13}$

$= 1x_1 + 3x_2 + 1x_3 + \cdots + 3x_{i-1} + x_i + 3x_{(i+1)} + \cdots + 1x_{11} + 3x_{12} + 1x_{13} + y_i - x_i$

$\equiv 0 + y_i - x_i (mod\ 10)$

Since $x_i \neq y_i$ and $0 \leq x_i, y_i \leq 9$, we find that
$y_i - x_i \not\equiv 0 (mod\ 10)$
Likewise, if i is even, then
(1,3,1,3,1,3,1,3,1,3,1,3,1).$(y_1 y_2 y_3 y_4\, y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12} y_{13})$
$\equiv 0 + 3(y_i - x_i)(mod\ 10)$
$\not\equiv 0(mod\ 10)$.
Hence $y_1 y_2 y_3 y_4\, y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12} y_{13}$ is not a correct UPC.

We now consider the following example:
Suppose a correct UPC for some product is 0023942874102
During typing in a computer, the following number has been typed 0029342874102, as a UPC. Then the computer will calculate
$1.0 + 3.0 + 1.2 + 3.9 + 1.3 + 3.4 + 1.2 + 3.8 + 1.7 + 3.4 + 1.1$
$+3.0 + 1.2$
$= 0 + 2 + 27 + 3 + 12 + 2 + 24 + 7 + 12 + 1 + 2$
$= 92 \not\equiv 0(\text{mod } 10)$.
Hence the computer will indicate that there is an error.
Notice that in this case the error is due to interchange of the adjacent digits 3 and 9. The error is detected here. Also note that $[3 - 9] \neq 5$.

Suppose now the following number has been typed 0023492874102
Since this is not a correct UPC it should not satisfy the congruence

$$1.0 + 3.0 + 1.2 + 3.3 + 1.4 + 3.9 + 1.2 + 3.8 + 1.7 + 3.4 + 1.1$$

$+3.0 + 1.2 \equiv 0(\text{mod } 10)$
But
L.H.S.$= 0 + 0 + 2 + 9 + 4 + 27 + 2 + 24 + 7 + 12 + 1 + 2$
$= 90 \equiv 0\ (\text{mod } 10)$.
So, the error is not detected here.
Observe that in this case the error is due to interchange of the adjacent digits 9 and 4, and $[9 - 4] = 5$.

From the above example we observe that the undetected transposition errors of adjacent digits a_i, and a_{i+1}. arise when $|a_i - a_{i+1}| = 5$. This we prove the following:

Theorem 7. In a UPC a transposition error of the form $a_1a_2 \dots a_ia_{i+1} \dots a_{13} \rightarrow a_1a_2 \dots a_{i+1}a_i \dots a_{13}$, as is undetected if and only if $|a_i - a_{i+1}| = 5$.

Proof. Suppose $a_1a_2 \dots a_ia_{i+1} \dots a_{13} \rightarrow a_1a_2 \dots a_{i+1}a_i \dots a_{13}$ If the changed UPC is correct, then either

$1a_1 + 3a_2 + \cdots + 1a_{i+1} + 3a_i + \cdots + 1y_{11} + 3y_{12} + 1y_{13}$

$\equiv 0(mod\ 10) \dots \dots (\text{i})$

$or, 1a_1 + 3a_2 + \cdots + 3a_{i+1} + 1a_i + \cdots + 1y_{11} + 3y_{12} + 1y_{13}$

$\equiv 0(mod\ 10) \dots \dots (\text{ii})$

according as i is odd or even.

Since $a_1a_2 \dots a_ia_{i+1} \dots a_{13}$ is a correct UPC, then corresponding to (i)

$1a_1 + 3a_2 + \cdots + 1a_{i+1} + 3a_i + \cdots + 1y_{11} + 3y_{12} + 1y_{13}$

$\equiv 0(mod\ 10)$

or, corresponding to (ii)

$1a_1 + 3a_2 + \cdots + 3a_{i+1} + 1a_i + \cdots + 1y_{11} + 3y_{12} + 1y_{13}$

$\equiv 0(mod\ 10)$

We find that $2|a_i - a_{i+1}| \equiv 0(mod\ 10)$.

If $a_i \neq a_{i+1}$, $0 < |a_i - a_{i+1}| < 10.$ Hence this holds if and only if $|a_i - a_{i+1}| = 5$. So, the error is undetected if and only if $|a_i - a_{i+1}| = 5$.

CONCLUSION

In this project I have explained the topic CONGRUENCE AND IT'S APPLICATIONS by providing many details on it. This project also emphasizes on main ideas related to the topic.

I took the ideas and research about this topic from the books and websites which are mentioned in the bibliography. I hope this project will be meaningful and effective to you

Bibliography

B.C. Chakraborty and M.K. Sen	Introduction to discrete mathematics, Fourth edition.
D.M. Burton	Elementary number theory, Second edition.
S.K. Mapa	Higher algebra: Classical, Ninth edition.
	https://www.isbn.org/about_isbn_standard#:~:text=When%20participating%20in%20the%20ISBN,ISBNs%20are%2013%2Ddigits%20long.