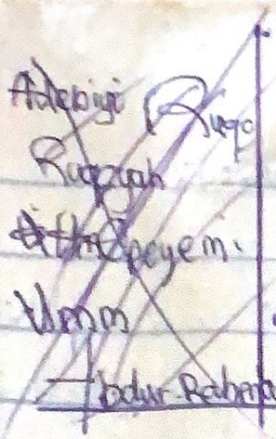

Number Theory and method of Proof:

Use definition of even and odd to justify these:

a) is 0 even b) is -301 odd c) If a & b are integer, is $6a^2b$ odd?

d) If a & b are integer, is $10a+8b+1$ odd?

e) is every integer either even or odd?

Solution:

Recall that: n is even iff, $n=2k$, (for every integer k).

n is odd iff $n=2k+1$, (for every integer k).

a) is 0 even $k=0$ $0 \in \mathbb{Z}$

$\therefore n=2k$, $2(0)=0$ $\therefore$ 0 is an even number.

b) is -301 odd., $k=-151$

$n=2k+1 = 2(-151)+1 = -302+1 = -301$. $\therefore$ -301 is odd.

c) is $6a^2b$ odd?

$n=2k+1$ $6a^2b = 2(3a^2b)$ and $n=2k$ (even).

$n=2(3a^2b)+1 = 6a^2b+1$,

$\therefore 6a^2b$ is an even.

d) $10a+8b+1$ is odd

$n=2k+1 = 2(5a+4b)+1 = 10a+8b+1$

$\therefore 10a+8b+1$ is an Odd number.

* Theorem: The sum of two even integers is even.

Suppose a & b are integers, Note: $\therefore (p+a)=t$

$a=2p$ $\therefore$ recall for even $\therefore$ $a+b=2p+2a$

$b=2a$ $n=2k$ $a+b=2(p+a)$

$\therefore$ Sum of two even integers = 2t. for

2) Prove that if n is an integer and n^2 is odd, then n is odd.

7) Show that the diff. of any odd integers and any even integer is odd

Solution.

Odd integer $a = 2p+1$

even integer $b = 2q$

∴ the diff.

$a - b$

$\therefore (2p+1) - 2q$

$2p+1-2q = 2p-2q+1$

$= 2(p-q)+1$

$\because p+q = t \therefore = -2t+1$.

$\therefore -2t+1$ is odd.

3) Show that for every odd integer n, n^2 is odd. If n is odd then n^2 is odd.

Goal: n^2 is odd

$\therefore n = 2k+1$

$\therefore n^2 = (2k+1)^2$

$= (2k+1)(2k+1)$

$= 4k^2+4k+1$

$= 4k^2+2k+2k+1$

$= 2k(2k+1)+1(2k+1)$.

$= 2k+1)4(2k+1)$

$2(2k^2+2k)+1$

$t = 2k^2+2k$

$\therefore n = 2t+1$

Proof by contradiction:

Rational Number.

A number S is rational there exists an integer a and $b \neq 0$ such that $S = a/b$. If a number is not rational is said to irrational.

(a) 1/2 (b) 2/3 (c) 7/3 (d) $q/3$

(e) 1/1 (f) 9/2 (g) 0 (h) 5 (i) 0.5

(j) $(m+n)/mn$, when $m, n \in Z$, $m \neq 0, n \neq 0$

Theorem: Every integer is a rational number.

Example: Show that any sum of rational number is rational

Solution

Let r and s be rational number.

$r = a/b$ for some $a, b \in Z$, $b \neq 0$.

$s = c/d$ for some $c, d \in Z$, $d \neq 0$

$r+s = \frac{a}{b} + \frac{c}{d}$

$= \frac{ad+bc}{bd}$

$= \frac{p}{q}$, when $p = (ad+bc)$,

therefor $r+s$ is

Example:

$\pi, \sqrt{2}, \sqrt{x}$, such that perfect square.

Example.

Show that $\sqrt{2}$ is ir

Solution.

let $\sqrt{2}$ be ration

$\exists p, q \in Z, q \neq 0$

$\sqrt{2} = \frac{p}{q}$ (this

$2 = \frac{p^2}{q^2}$

$2q^2 = p^2$

p is even

$2q^2 = (2m)^2$

$2q^2 = 4m^2$

$q^2 = 2m^2$

q^2 is even

$(2n)^2 = 2m^2$

$4n^2 = 2m^2$

$2n^2 = m^2$, m

q is even.

$\frac{p}{q}$, where $p = (ad+bc)q - bd$.

therefor $r + s$ is rational

* ~~Example~~:

$\pi, \sqrt{2}, \sqrt{x}$, such that x is non perfect square.

~~Example~~.

Show that $\sqrt{2}$ is irrational

Solution:

let $\sqrt{2}$ be rational.

$\exists p, q \in Z, q \neq 0$

$\sqrt{2} = \frac{p}{q}$ (p & q has no common factor)

$2 = \frac{p^2}{q^2}$

$2q^2 = p^2$, p^2 is even,

p is even

$2q^2 = (2m)^2$

$2q^2 = 4m^2$

$q^2 = 2m^2$

q^2 is even, then q is even

$(2n)^2 = 2m^2$

$4n^2 = 2m^2$

$2n^2 = m^2$, m^2 is even, m is also even.

$\therefore 2n^2 = (2r)^2$ for some

$2n^2 = 4r^2$

$n^2 = 2r^2$

$\therefore$ therefore $\sqrt{2}$ is irrational.

exclusive.

~~Exclusive proof~~

Example: Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution

$(n+1)^3 \geq 3^n \quad n \leq 4$

$(1, 2, 3, 4)$

when $n=1$, $(n+1)^3 = (1+1)^3 = 8$

$\therefore 8 \geq 3$

when $n = 2$

$(2+1)^3 = 27 \geq 9$

when $n = 3$

$(3+1)^3 = 64 \geq 27$

when $n = 4$

$(4+1)^4 = 125 \geq 81$

Hence $(n+1)^3 \geq 3^n$, when $n \geq 4$, and $n \in Z^+$.

Proof by cases.

Example: prove that if n is an integer, then $[n^2 \geq n]$

Solution

there are 3 cases, $n=0$, $n>0$, $n<0$

Case 1: when $n=0$, $0^2 \geq 0$, therefore true.

case 2: when $n \geq 1$, $1^2 \geq 1$, therefore $n^2 \geq n$ (tr

case 3: when $n \leq -1$, we note that $n^2 \geq n$ is ca

therefore $n^2 \geq n$

Uniqueness Proofs.

Example: show that if a and b are real numb

$a \neq 0$ then there is a unique real no such that

$ar + b = 0$

Soln:

firstly, we find the real number.

we note that $r = -b/a$ is soln to $ar + b = 0$

$a\left(\frac{-b}{a}\right) + b = -b + b = 0$

Consequently, $ar + b = 0$ has solution $r = -b/a$

secondly, suppose $ar + b = 0$, has solution s

$ar + b = 0$

$as + b = 0$

$ar + b = as + b$

$ar = as$

$r = s$

Prime and Compo

Def:

$n > 1$ is prime iff

$n = rs$

then either $r = 1$

$n > 1$ is composite

$1 < r < n$ and

(a) 2 (b) 3 (c)

Example: is

Soln. 2 cannot

3 ✓

5 ✓

7 ✓

11 ✓

Example: Prove

that can be

of two prime

Soln: $n =$

1st $20 = 17$

$20 = 13$

Ex: suppose th

there exists

$= 2k$.

Soln: show

false - there

is a prime

Prime and Composite Numbers:

Def:

$n>1$ is prime iff $\forall r, s \in \mathbb{Z}$ if $n = rs$ then either $r=1$ and $s=n$ or $r=n$ and $s=1$

$n>1$ is composite iff $\exists r, s \in \mathbb{Z}$ if $n=rs$ then $1<r<n$ and $1<s<n$.

(a) 2 (b) 3 (c) 1

Example: Is 67 prime?

Soln. 2 cannot devide 67 ... 67
3 ... 67 ... 67
5 ... 67 ... 67
7 ... 67 ... 67
11 ... 67 ... 67

Example: Prove that there exists an even integer n that can be written in two ways as a sum of two prime numbers.

Soln: $n = 20$

1st $20 = 17 + 3$

$20 = 13 + 7$

Ex: Suppose that r and s are integer Prove that there exist an integer k such that $22r + 185 = 2k$.

Soln: Show that the following sta... false - there is positive integer n such that ... a prime.

n^2+3n+2 is composite.

$n^2+3n+2 = n^2+n+2n+2$.

$= n(n+1)+2(n+1)$

$= (n+1)(n+2)$.

$n^2+3n+2 = (n+1)(n+2) = rs$.

Claim: $r = (n+1)$, $s = (n+2)$

We note that $(n+1) > 1$ $(n+1) < (n^2+3n+2)$

$1 < (n+1) < (n^2+3n+2)$

$\therefore 1 < (n+2) < (n^2+3n+2)$.

$\therefore n^2+3n+2$ is not prime.

The fundam

$\forall a \in Z$

$a = p$

where

p_i

Example:

1) 100

2 | 100

2 | 50

5 | 25

5 | 5

1

100 =

=

The fundamental Theorem of Arithmetic.

$\forall\ a \in \mathbb{Z};\ a > 1$

$a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_n^{a_n}$ ∃! unique.

Prime factorization.

where p_i's are prime factor of a

$p_1 < p_2 < p_3 < \cdots < p_n$.

Example: Obtain the prime factorization of.

1) 100 ② 641 ③ 999 ④ 1024.

2	100
2	50
5	25
5	5
	1

641	641
	1
	641 = 641¹

$999 = 3^3 \cdot 37^1$ $1024 =$

$100 = 2, 2, 5, 5$

$= 2^2 \cdot 5^2$

Divisibility:

If $n, d \in \mathbb{Z}$,

d divides n, iff $\exists\ k \in \mathbb{Z}$, i.e $n = dk$

d divides n is denoted by d/n.

If e does not divide n we write $d \nmid n$.

Examples Determine whether 3/7 and whether 3/12.

Sol:

ⓐ 3×7

ⓑ $3/12$ → true.

Theorem: let a, b and c be integers where a ≠ 0
then
i) If a|b and a|c, then a|(b+c)
ii) If a|b, the a|bc
iii) If a|b and b|c then a|c.

Proof

i) let a|b and a|c
∃ m, n ∈ ℤ such that
b = am and c = an
By definition of divisibility.
Add ① and ②
(b+c) = am + an
(b+c) = (m+n)a
= ka, where k = m+n; k ∈ ℤ
b+c = ka
Therefore: b+c = ka
a|(b+c) = k.

ii) Suppose a|b
⇒ b = sa, for some integer s.
If we multiply both sides by c ∈ ℤ
cb = csa
cb = ka, where k = cs
therefore k = cb/a or a|cb.

iii) Suppose a|b and b|c
∃ m, n ∈ ℤ such that b
c = nb = n(ma).
c = (nm)k.
a|c

Example Is the following statem
b|a, then a = b?
Solution.
(a) True (b) false. (Due to
The Division Algo
Given any integer n an
then ∃ q, r ∈ ℤ su
n = dq + r
(dividor) (quotient) (remainder).

Example. Find integer q and r
(a) n = 54, d = 4.
(b) n = 54, d = 70
Sol.
n = dq + r
54 = 4(q) + r
13
54 = 4(13) +
therefore q = 13, r =

(ii) Suppose $a|b$ and $b|c$

$\exists m, n \in \mathbb{Z}$ such that $b = ma$ and $c = nb$

$c = nb = n(ma)$.

$c = (nm)a$.

$a|c$

Example Is the following statement true, if $a|b$ and $b|a$, then $a = b$?

Solution.

(a) True (b) false. (due to the sign Counterexample)

The Division Algorithm.

Given any integer n and positive integer d, then $\exists\ q, r \in \mathbb{Z}$ such that

$n = dq + r \qquad 0 \le r < d$

(divisor) (quotient) (remainder).

Example. Find integer q and r such that $n = dq$

(a) $n = 54$, $d = 4$.

(b) $n = 54$, $d = 70$

Sol.

$n = dq + r$

$54 = 4(q) + r$

$54 = 4(13) + 2$

Therefore $q = 13$, $r = 2$.

ii) $n = -54$, $d = 4$.

$n = dq + r$

$-54 = 4(q) + r$

$+ \quad -14 \quad 2$

$-54 = 4(-14) + 2$

$\therefore q = -14, r = 2$.

iii) $n = 54$, $d = 70$

$54 = 70(q) + r$

$0 \quad 54$

$54 = 70(0) + 54$.

$\therefore q = 0, r = 54$.

Modular Arithmetic.

n div $d \Rightarrow \frac{n}{d} = q$ and r

Example modulo

$n \bmod d = r$ iff

$n = dq + r$

54 mod 4 = 2

5 mod 4 = 1

7 mod 9 = 7

$a \equiv b \bmod m$ iff

$m/(a-b)$

Exam Determine if 17 is congruet to 5 modulo 6 and whether 28 and 14 are congruet

≡ congruet

solution

$17 \equiv 5 \bmod 6$, True?

a b m

$a - b = 17 - 5 = 12$, de

then $17 = 5 \bmod 6$

Alter:

$17 \bmod 6 = 5$.

$5 \bmod 6 = 5 = 17 \bmod 6$

$\therefore 17 \equiv 5 \bmod 6$.

ii) $a = 28$, $b = 14$, $m =$

$(a - b) = 28 - 14 = 14$.

therefore 28 is not

$m/(a-b)$

$a \equiv b \pmod m$ iff

$a \bmod m = b \bmod m$

$17 \bmod 6$

$5 \equiv$

$28 \bmod 6$

$4 =$

2^2

2^4

≡ congruet

solution

$17 \equiv 5 \bmod 6$, True?

a b m

$a - b = 17 - 5 = 12$, clearly $6 \mid 12$

then $17 = 5 \bmod 6$

Alter:

$17 \bmod 6 = 5$.

$5 \bmod 6 = 5 = 17 \bmod 6$.

$\therefore 17 \equiv 5 \bmod 6$.

ii) $a = 28$, $b = 14$, $m = 6$

$(a - b) = 28 - 14 = 14$. $6 \mid 14$ 6×14.

therefore 28 is not congruet to $14 \bmod 6$.

$m \mid (a - b)$

$a \equiv b \pmod m$ iff

$a \bmod m = b \bmod m$.

$17 \bmod 6 = 5 \bmod 6$.

$5 \equiv 5$. 2 1

$28 \bmod 6 \equiv 14 \bmod 6$.

4 =

$2 \quad 2$

2^2

6×14.

Theorem: Let m be a positive integer, The integers a and b a
Congruet to m if and only if there exists integer k
Such that $a = b + km$.

proof: Suppose $a \equiv b \bmod m$

by definition $m|(a-b)$

$\Rightarrow a - b = km$ for some $k \in \mathbb{Z}$.

Hence, $a = b + km$.

Conversely, assume $a = b + km$

$a - b = km$.

$= m|(a-b)$

$\Rightarrow a \equiv b \pmod m$

Theorem: Let m be a positive integer. If $a \equiv b \pmod m$ an
$c \equiv d \pmod m$ Then

$(a+c) = (b+d) \bmod m$ and.

$ac = bd \pmod m$

proof: $a \equiv b \pmod m$ and $c \equiv d \pmod m$

by theorem Above $a = b + sm$ and $c = d + tm$,

$a + c = (b + sm) + (d + tm)$

$= (b+d) + (s+t)m$

$= (b+d) + km$, for $k = s + t$ $k \in \mathbb{Z}$.

Therefore, $(a+c) \equiv (b+d) \bmod m$.

$a \equiv b \pmod m$, c

Suppose $a = b +$

$a \cdot c = (b + sm)(c$

$ac = (bd)(sm$

$ac = bd(st)m$

$ac = (bd)km$ wo

$\therefore ac \equiv (bd) \bmod m$

Example...

Corollary, Let m b

$(a+b) \bmod m =$

$(ab) \bmod m = ($

Example: find the

Solution: $(19^3$

19^3 mod

$(19^3 \bmod 3$

40

Hence, $(19^3$

Greg

Let a an

The larget

is caued

a and b a

$a \equiv b \pmod m$, $c \equiv d \pmod m$

Suppose $a = b + sm$, $c = d + tm$ $s, t \in \mathbb{Z}$.

$a \cdot c = (b + sm)(d + tm)$

$ac = (bd)(sm \cdot tm)$.

$ac = bd(st)m$.

$ac = (bd)km$ where $k = st$ $k \in \mathbb{Z}$.

$\therefore ac \equiv (bd) \bmod m$.

~~Example...~~

★ Corollary, Let m be a positive integer. Then

$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

Example: Find the value of $(19^3 \text{ and } 31)^4 \bmod 23$.

Solution: $(19^3 \bmod 31)^4 \bmod 23$.

$19^3 \bmod 31 = 6859 \bmod 31 = 8$

$(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23 = 4096 \bmod 23$

$4096 \bmod 23 = 2$.

Hence, $(19^3 \bmod 31)^4 \bmod 23 = 2$.

Greatest Common Divisor (GCD)

Let a and b be integers not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b and is denoted by $\gcd(a, b) = d$.

If $c|a$, $c|b$, ... $c < d$

gcd (Greatest Common divisor).

Example:

Find the gcd(a,b)

i) a = 27, b = 72 ii) a = 72, b = 63, iii) a = 7, b = 3

Solution: Solution Solution

gcd(a,b) = d. gcd(a,b) = d gcd(a,b) = d

gcd(27,72) = 9 gcd(72,63) = 9 gcd(7,3) =

Definitions

1) Integer a and b are relatively prime if:

$$\gcd(a,b) = 1$$

2) Integers a_1, a_2, a_3, a_n are pairwise relatively prime if $\gcd(a_i, a_j) = 1$, whenever $1 \le i < j \le n$.

Example:

1) Integer 7 and 3 are r.p because

$$\gcd(7,3) = 1$$

2) Integers 4 and 9 are rp because

$$\gcd(4,9) = 1$$

3) Determine whether Integer 10, 17 and 21 are pairwise relatively Prime. and 10, 19 and 24, 24 are Pairwise relatively Prime.

Solution

10, 17 and 21

gcd(10,17) = 1

gcd(10,21) = 1 and gcd(17,21) = 1 Pairwise.

Hence, the statement 10, 17 and 21 are r.p.

7) for Integers

Solution

gcd(10, 19)

gcd(10, 24

gcd(19, 24

Hence, the

Prim

a = P

gcd

Example:

72 = 2^3. 3

63 = 2^0. 3

P, P

gcd[72

gcd = 3

* lcm(a,b)

for In

2 | 24
3 | 12
4

2 | 10 | 3 | 21
5 | 5 | 3 | 9
1 | 1 | 3 | 3
1 | | 1 | 1

L Q.

2) for Integer 10, 19, 24.

Solution

$\gcd(10,19) = 1$

$\gcd(10,24) = 2$.

$\gcd(19,24) = 1$

Hence, the Set of Integer 10, 19, 24 is not pairwise r.p.

Prime factorization.

$$a = P_1^{\alpha_1} P_2^{\alpha_2} P_3^{\alpha_3} \cdots P_n^{\alpha_n}$$

$$\gcd(a,b) = P_1^{\min(\alpha_1, \beta_1)} P_2^{\min(\alpha_2, \beta_2)} \cdots$$

Example: $\gcd(72, 63)$

$72 = 2^3 \cdot 3^2 \cdot 4^0 \cdot 5^0 \cdot 6^0 \cdot 7^0$

$63 = 2^0 \cdot 3^2 \cdot 4^0 \cdot 5^0 \cdot 6^0 \cdot 7^1$

$P_1 \; P_2 \; P_3 \; P_4 \; P_5 \; P_6$

$\gcd(72,63) = 2^0 \cdot 3^2 \cdot 4^0 \cdot 5^0 \cdot 6^0 \cdot 7^0$

$\gcd = 3^2 = 9$

* $\text{lcm}(a,b) = P_1^{\max(\alpha_1,\beta_1)} P_2^{\max(\alpha_2,\beta_2)} \cdots P_n^{\max(\alpha_n,\beta_n)}$

for Integer a and b not equal zero

$ab = \gcd(a,b)\ \text{lcm}(a,b)$

The Euclidean Algorithm.

Let a and b be integers not both zero by division algorithm.

Theorem: $a = bq + r \quad 0 \le r < b$

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

Proof

Let $a = r_0, b = r_1$

$r_0 = r_1 q_1 + r_2 \quad 0 \le r_2 < r_1$

$r_1 = r_2 q_2 + r_3 \quad 0 \le r_3 < r_2$

$r_2 = r_3 q_3 + r_4 \quad 0 \le r_4 < r_3$

⋮

$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \le r_n < r_{n-1}$

$r_{n-1} = r_n q_n + 0$

Hence $\gcd(a,b) = r_n$. r_0 r_1

Example find $\gcd(47, 3)$ using E.A. (a, b)

Solution $a = bq + r$.

(1) $47 = (3)(15) + 2 \quad 0 \le 2 < 3$

$3 = (2)(1) + 1 \quad 0 \le 1 < 2$

$2 = (1)(2) + 0$

therefore $\gcd(47, 3) = 1$

(2) find $\gcd(414, 602)$ using the E.A.

$a = bq + r$. $\quad r_0 = 414, r_1 = 602$.

$\gcd(b,$

$\gcd(a,b) =$

$602 = 414(1)$

$414 = 188(2)$

$188 = 38(4)$

$38 = 36(1)$

$36 = 2(18)$

$\Rightarrow$ therefore

GCD as l

If a and b

integers s and

as +

Example: Express gcd(

Sol

$\gcd(7,3) = 1$

$as + bt = 1$

$7(1) +$

Therefore s

2) Express gc

as + bt

$602($

gcd(a,b) = gcd(b,a) ∴ gcd(414, 602) = gcd(602, 414)

602 = 414(1) + 188 $0 \leq 188 < 414$

414 = 188(2) + 38 $0 \leq 38 < 188$

188 = 38(4) + 36 $0 \leq 36 < 38$.

38 = 36(1) + 2. $0 \leq 2 < 36$.

36 = 2(18) + 0

∴ therefore gcd(414, 602) = 2.

GCD as linear Combination.

If a and b are positive Integers then ∃ Integers s and t such that

as + bt = gcd(a,b)

as + bt = d, where d = gcd(a,b).

Example: Express gcd(7, 3) as linear Combination.

Sol:

gcd(7,3) = 1

as + bt = 1

7(1) + 3(-2) = 1

Therefore s = 1, t = -2 Bezout is co-efficient

2) Express gcd(602, 414) = 2 as linear Combination,

as + bt = 2.

602( ) + 414( ) = 2.

$602 = 414(1) + 188$

$414 = 188(2) + 38 \quad 38 = 414 - 188(2)$

$188 = 38(4) + 36 \quad 36 = 188 - 38(4)$

$38 = 36(1) + 2 \quad 2 = 38 - 36(1)$

$36 = 2(18) + 0$

From Backward Substitution in E.A

$2 \Rightarrow 38 - 36(1) = 38 - (188 - 38(4)) = 38 - 188 + 4(38)$

$\Rightarrow 5(38) - 188 = 5(414 - 188(2)) - 188.$

$\Rightarrow 5(414) - 11(188)$

$\Rightarrow 5(414) - 11(602 - 414)$

$\Rightarrow 5(414) - 11(602) + 11(414)$

$= 16(414) + (-11)(602).$

Therefore $s = 16, t = -11.$

3) Express gcd(252, 198) as l.c - (linear combination)

$252 = 198(1) + 54. \quad 54 = 252 - 198(1)$

$198 = 54(3) + 36 \quad 36 = 198 - 54(3)$

$54 = 36(1) + 18. \quad 18 = 54 - 36(1)$

$36 = 18(2) + 0$

$18 = 54 - 36(1) = 54 - (198 - 54(3)) = 54 - 198 + 3(54)$

$= 4(54) - 198 = 4(252 - 198) + 198$

$= 4(252) - 4(198) - 198.$

$= 4(252) - 5(198)$

Hence, $s = 4, t = -5.$

Inverse Modulo m

x is an inverse of a modulo m if ax and 1 are congruent modulo m.

Example: Find an inverse of 3 modulo 7 multiplicative inverse.

Solution

$7 = 3(2) + 1$

$3 = 1(3)$

$\Rightarrow 1 = 7(1) + 3(-2)$

Proof $= -2$ is inverse of 3 mod.

the inverse of 3 mod 7 is 5

2) -2 inverse of 3 and 40

$40 = 3(13) + 1$

$13 = 13 = 13(1)$

$\Rightarrow 1 = 40 + 3(-13)$

Thus, -13 is the inverse of 3.

therefore 27 is the inverse of 3.

Linear Congruence.

$ax = b \pmod m$

$a^{-1}ax = a^{-1}b \pmod m$

$x = a^{-1}b \pmod m$

$ax = b \pmod m$

$a^{-1}x = a^{-1}b \pmod m$

$x = a^{-1}b \pmod m$

$a^{-1}a = 1 \pmod{n}$

Example: What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$

Solution:

$7 = 3(2) + 1$

$1 = 7 + 3(-2)$

Inverse of 3 is -2

$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$

$x \equiv -8 \pmod 7 \equiv -1 \pmod 7$

$\equiv 6 \pmod 7$

Then $x = 6$ and 7

Example

$\{1, 2, 6, 8, \ldots, 81, 1\}$

Solution, use inverse to solve:

$57k = 13$ and 67

$57 = (13)(4) + 5$

$13 = 5(2) + 3$

$5 = (3)(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2)$

Inverse of 57 is

$x = 59 \pmod{67}$

Chinese Remainder Theorem:

Theorem: Let $m_1, m_2, m_3 \ldots m_n$ be pair wise r.p positive integers greater than 1 and $a_1, a_2, a_3 \ldots a_n$ be integers then

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}.$$

has a unique solution modulo $M = m_1, m_1 \ldots m_n$ with $0 \leq x < m$.

Example: Find all integers x, $0 \leq x < 91$ such that

$$x \equiv 3 \pmod{7}$$
$$x \equiv 6 \pmod{13}$$

Solution:

$$M = m_1 m_2 = 7 \times 13 = 91$$

$$M_1 = \frac{M}{m_1} = \frac{91}{7} = 13, \quad M_2 = \frac{M}{m_2} = \frac{91}{13} = 7$$

Find $x_1 =$ $\quad x_2 =$

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 = 45.$$

$$x = 45 \text{ and } 91$$

Example: Solve the linear Congruences.

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Soln

$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3$.

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$.

$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$.

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$.

$X_1 = 35^{-1} \pmod 3 = 2^{-1} \pmod 3 = 2$

$X_2 = 21^{-1} \pmod 5 = 1^{-1} \pmod 5 = 1$

$X_3 = 15 \pmod 7 = 1^{-1} \pmod 7 = 1$

$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 2 \cdot 15 \cdot 1$

$= 140 + 63 + 30$

$= 233 \equiv 23 \pmod{105}, \quad 0 \leq x < 105$

Therefore, 23 is the smallest positive integer that satisfies the linear Congruences.

Recu

Example:

$n = 1, \quad a_1 =$

$n = 2, \quad a_2 =$

$n = 3, \quad a_3 =$

$n = 4, \quad a_4 =$

$n = 5, \quad a_5 =$

Examp: f

find f_6

$f_0 = 0, \quad f_1 =$

$f_2 = f_0 + f_1$

$f_3 = f_2 + f$

$f_4 = f_3 +$

$f_5 = f_4 +$

$f_6 = f_5 +$

$\therefore f_6 =$

Example:

{an} sa

Solution

an

Soln: S

recurrenc

Recurrence Relations.

Example: $a_n = na_{n-1}$, $a_1 = 1$

$n=1$, $a_1 = 1$

$n=2$, $a_2 = 2a_1 = 2 \cdot 1 = 2$.

$n=3$, $a_3 = 3a_2 = 3 \cdot 2 \cdot 1$

$n=4$, $a_4 = 4a_3 = 4 \cdot 3 \cdot 2 \cdot 1$

$n=5$, $a_5 = 5a_4 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Examp: $f_n = f_{n-1} + f_{n-2}$, $f_0 = 0$, $f_1 = 1$

find f_6

$f_0 = 0$, $f_1 = 1$

$f_2 = f_0 + f_1 = 0 + 1 = 1$

$f_3 = f_2 + f_1 = 1 + 1 = 2$.

$f_4 = f_3 + f_2 = 2 + 1 = 3$.

$f_5 = f_4 + f_3 = 3 + 2 = 5$

$f_6 = f_5 + f_4 = 5 + 3 = 8$.

$\therefore f_6 = 8$ $F_6 = 0, 1, 1, 2, 3, 5, 8 \ldots$.

* Example: Determine whether the sequence $\{a_n\}$ where $a_n = 3n$ for $n = 1, 2, 3 \ldots$ is a solution to the recurrence relation

$a_n = 2a_{n-1} - a_{n-2}$.

Soln: Suppose $a_n = 3n$ is a soln to the recurrence relation. $a_{n-1} = 3(n-1)$ and $a_{n-2} = 3(n-2)$

but $a_n = 2a_{n-1} - a_{n-2} = 3(3(n-1)) - 3(n-2) =$

$6n - 6 - 3n + 6$

$= 3n = a_n$

The method iteration:

Example: Solve the recurrence relation.

$a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$ and $a_1 = 2$

Solu

$a_1 = 2$

$a_2 = a_1 + 3 = 2 + 3$ $\quad 2 + 3 \cdot 1$

$a_3 = a_2 + 3 = 2 + 3 + 3$ $\quad 2 + 3 \cdot 2$

$a_4 = a_3 + 3 = 2 + 3 + 3 + 3$ $\quad 2 + 3 \cdot 3$

$\vdots$

$a_n = a_{n-1} + 3 = \underbrace{2 + 3 + 3 + \cdots + 3}_{(n-1)} = 3 + 3(n-1)$

Hence, $a_n = 2 + 3(n-1)$ is solution to

$a_n = a_{n-1} + 3$.

* Example: Solve $m_k = 2m_{k-1} + 1$, for $k = 1, 2$

$m_1 = 1$

Solu

$m_1 = 1$

$m_2 = 2m_1 + 1 = 2 \cdot 1 + 1$

$m_3 = 2m_2 + 1 = 2(2+1) + 1 = 2^2 + 2 + 1$

$m_4 = 2m_3 + 1 = 2($

$m_5 = 2m_4 + 1 = 2($

!

$m_n =$

$a = 1, r = 2$ $\quad = 1$

$= \frac{a(r^n - 1)}{r - 1}$

$m_n = 2^n - 1$

Hence, $m_n = 2^n - 1$