SPEED

Spring 2019

Session 9

Credit Hour System

Discrete Math Number Theory

SPEED TEL

SPEED COPY

Discrete math (9)

Number theory

*Division:-

If $a, b \in \mathbb{Z}$, $a \neq 0$: $a \mid b$ if $\frac{b}{a}$ = integer

a divides b

a is a factor of b & b is multiple of a

b is divisible by a

Ex:

how many +ve integers not exceeding n are multiples of d for $n, d \in \mathbb{Z}^+$?

Sol:-

positive multiple of d is kd (k: +

$$0 < kd \leq n$$

$$0 < k \leq \frac{n}{d}$$

k is integer, so : $0 < k \leq \lfloor \frac{n}{d} \rfloor$

number of +ve multiplies of d not exceeding n is $\left\lfloor \frac{n}{d} \right\rfloor$

* Properties of Division:

If $a, b, c \in \mathbb{Z}$:

1) If $a|b$ and $a|c$ then $a|(b+c)$

$\frac{b}{a}$

$a | \lfloor b+c \rfloor$

2) If $a|b$ then $a|bc$

$a | \lfloor b+c \rfloor$

3) If $a|b$ and $b|c$ then $a|c$

$a | \lfloor b+c \rfloor$

4) If $a|b$ and $a|c$ then $a|(mb+nc)$, for $m, n \in \mathbb{Z}$

$\frac{a}{d} = q + \frac{r}{d}$ remin

$\frac{a}{d} = q + \frac{r}{d}$ remin

* Quotient and Remainder:-

$\frac{a}{d} = q + \frac{r}{d}$

$\frac{a}{d} = q + \frac{r}{d}$ rem

Let $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$

$$\boxed{\frac{a}{d}} = \boxed{q + \frac{r}{d}}$$

remainder

quotient

$[q, r : \text{int}, \ 0 \leq r < d]$

To calculate q, r:

$$q = \lfloor \frac{a}{d} \rfloor \ , \ r = a - q * d$$

proof of existance of q, r:

if we take $q = \lfloor \frac{a}{d} \rfloor$, $r = a - qd$

int

, we need to prove that $0 \leq r < d$

$$\frac{a}{d} - 1 < \lfloor \frac{a}{d} \rfloor \cancel{\leq \frac{a}{d}}$$

$$a - d < \lfloor \frac{a}{d} \rfloor d \leq a$$

$\downarrow * -1$

$$-a \leq -\lfloor \frac{a}{d} \rfloor d < d - a$$

$+a$

$$a - a \leq \boxed{a - \lfloor \frac{a}{d} \rfloor d} < d - a + a$$

$$0 \leq r < d$$

proof of uniqueness:

Let we have 2 pairs (q_1, r_1), (q_2, r_2)

that satisfy:

$a = q_1 d + r_1$, $0 \le r_1 < d$

$a = q_2 d + r_2$, $0 \le r_2 < d$

$\therefore q_1 d + r_1 = q_2 d + r_2$

$(q_1 - q_2) d = r_2 - r_1$

case 1:

$q_1 = q_2$ and so $0 = r_2 - r_1$

$\therefore r_2 = r_1$ [unique q, d]

case 2: assume without loss of generality

$q_1 > q_2$

$\therefore q_1 = q_2 + n$

$\therefore n d = r_2 - r_1 \longrightarrow r_2 = r_1 + n d$

if one of r_1, r_2 satisfy $0 \leq r < d$
the other won't satisfy this Condition

So there exist unique integers q, d
that satisfy:

$$a = qd + r$$

* Modular congruence:

$$a \equiv b \pmod{m} \quad \text{if } m \mid a-b$$

$$\frac{a-b}{m} = \text{integer}$$

$a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

note:

- Congruence modulo m is an equivalence relation
- $a \equiv b \bmod m$ iff $a \bmod m = b \bmod m$
- $a \equiv b \bmod m$ iff there is $k \in \mathbb{Z}$ such that $a = b + km$

properties :-

Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

1) If $a \equiv b \bmod m$, $c \equiv d \bmod m$

then $(a+c) \equiv (b+d) \bmod m$

& $ac \equiv bd \bmod m$

2) $(a \bmod m) \bmod m = a \bmod m$

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

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

Example :

Find $(a+b) \bmod 26$, $ab \bmod 26$

if $a \bmod 26 = 12$, $b \bmod 26 = 6$

Sol:- $((a \bmod 26) + (b \bmod 26)) \bmod 26$

$(18) \bmod (26)$

$(a+b) \bmod 26 = (a \bmod 26 + b \bmod 26) \bmod 26$

$= (12+6) \bmod 26 = 18$

$ab \bmod 26 = ((a \bmod 26)(b \bmod 26)) \bmod 26$

$= (12 * 6) \bmod 26$

$= 72 \bmod 26$

$= 20$

* Prime numbers:-

an integer $p > 1$ is prime if the only the factors of p are $1, p$. otherwise, p is composite

Example:

what are the prime numbers not exceeding 100?

Sol:-

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89,

* The

If

incre

prim

$\boxed{n =}$

The

Prim

* Theo

Let

-If n

of n

facto

*The Fundamental theorem of Arithmetic:

If $n \in \mathbb{Z}^+$, then there is a unique increasing sequence $P_1, P_2, \dots P_m$ of primes, $(m \geq 1)$ such that

$$\boxed{n = P_1 P_2 \cdots P_m}$$

The sequence $P_1, P_2, \dots P_m$ is the prime factorization of n

*Theorem:-

Let $n \in \mathbb{Z}^+$

-If $n = ab$, then the prime factorization of n is the result of merging the prime factorizations of a, b

- If p is a prime, $p \mid n$ and $P_1, P_2, \ldots P_m$ is the prime factoriz of n, then $p = P_i$ for some $1 \leq i \leq m$

Example:-

Find the prime factorization of 100

Sol:-

$\frac{100}{2} = 50$

$\frac{50}{2} = 25$

$\frac{25}{2} \neq$ integer

$\frac{25}{3} \neq$ integer

$\frac{25}{5} = 5$

$\frac{5}{5} = 1$

$\therefore \quad 100 = 2^2 * 5^2$

$\frac{100}{2} = 50$

$\frac{50}{2} = 25$

$\frac{25}{2} \times$

$\frac{25}{5}$ 5

$\frac{5}{5}$ 1

Theorem:

If n is a Composite, then n has prime factors Less than or equal to $\sqrt{n}$.

Proof:-

Let $n = ab$

assume $a > \sqrt{n}$, $b > \sqrt{n}$

$ab > n$ (Condi tradication)

So $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

assume without Loss of generality

$a \leq \sqrt{n}$

if a is prime, then the proof is done

Else a has a factor $p < a \leq \sqrt{n}$

p is a factor of a , a is a factor of n

$\therefore$ p is a factor of n

prime

$\therefore$ n has a prime factor $p < \sqrt{n}$

*Theorem:-

There are infinitely many primes

Proof:

assume there is finite number of primes

then there is some $m \in \mathbb{Z}$ such that

$P_1, P_2, \ldots P_m$ are the all primes

the max prime is P_m

Let $n = P_1 P_2 \ldots P_m + 1$

$n > P_i \ (1 \leq i \leq m)$

$n > P_m$

$\therefore$ n is not prime

$\therefore$ there exist P_j such that $P_j \mid n$

but $P_j \mid P_1 P_2 \cdots P_m$

$\therefore$ $P_j \mid n - P_1 P_2 \cdots P_m$

$P_j \mid 1$ [Contradication as P is prime $(P > 1)$]

$\therefore$ There are infinitely many primes

$n > P_i \ (1 \leq i \leq m)$

$n > P_m$

$\therefore$ n is not prime

$\therefore$ there exist P_j such that $P_j \mid n$

but $P_j \mid P_1 P_2 \cdots P_m$

$\therefore$ $P_j \mid n - P_1 P_2 \cdots P_m$

$P_j \mid 1$ [Contradication as P is prime $(P > 1)$]

$\therefore$ There are infinitely many primes

* Greatest common divisor:-

gcd (a, b) is the Largest int d

Such that $d \mid a$ and $d \mid b$

If gcd (a, b) = 1, then a, b are relatively prime.

Theorem:-

Let $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$

If F_a and F_b are respectively the prime factorization of a and b, the the prime factorization of gcd (a, b) the Longest common subsequence of F_a and F_b

proof:-

Let F be the Longest Common Subsequence of F_a and F_b

The integer d whose prime factorization is F, divides both a, b

$d \mid a$, $d \mid b$

let $c > d$; c is a common factor of a, b

$\therefore$ c must have a prime factor $\notin F$

but the prime factors of c are common factors of a, b and so

prime factors of $c \in F$ (which is contradication)

$\therefore$ The proof is done

$\frac{120}{2}$ 60 $\quad 2^3\ 3\ 5 \quad$ $\frac{500}{2}$ 250

$\frac{60}{2}$ 30 $\quad$ $\frac{250}{2}$ 125

$\frac{30}{2}$ 15 $\quad$ $\frac{125}{5}$ 25

$\frac{15}{3}$ 5 $\quad$ $\frac{25}{5}$ 5

$\frac{5}{5}$ 1 $\quad$ $\frac{5}{5}$ 1

$5^3\ 2^2$

Example :-

Find GCD of 120 and 500?

Sol:-

$\frac{120}{2} = 60$ $\qquad$ $\frac{500}{2} = 250$

$\frac{60}{2} = 30$ $\qquad$ $\frac{250}{2} = 125$

$\frac{30}{2} = 15$ $\qquad$ $\frac{125}{2} \neq int$

$\frac{15}{2} \neq int$ $\qquad$ $\frac{125}{3} \neq int$

$\frac{15}{3} = 5$ $\qquad$ $\frac{125}{5} = 25$

$\frac{5}{3} \neq int$ $\qquad$ $\frac{25}{5} = 5$

$\frac{5}{5} = 1$ $\qquad$ $\frac{5}{5} = 1$

$120 = 2^3 * 3 * 5$ $\qquad$ $500 = 2^2 * 5^3$

min

$gcd(120, 500) = 2^2 * 5 = 20$

* Least common multiple:-

Lcm(a,b) is the least int m such that $a|m$, $b|m$

Theorem:

If $a, b \in Z^+$ then

$$\boxed{ab = \gcd(a,b)\ \mathrm{Lcm}(a,b)}$$

Ex:

Find Lcm of 120, 500?

Sol:

max

$$\mathrm{Lcm}(120, 500) = \frac{120 * 500}{\gcd(120,500)}$$

$$= \frac{120 * 500}{20}$$

$$\boxed{5^3\ 2^3\ 3}$$

$$= 3000$$

Example :-

Find the greatest common divisor of the following pairs of integers:

1) 24 and 36

2) 112 and 64

3) 45 and 0

4) 10 and 21

5) 12 and 22

Sol:-

1) $24 = 2^3 * 3$, $36 = 2^2 * 3^2$

$gcd(24, 36) = 2^2 * 3 = 12$

2) $112 = 2^4 * 7$, $64 = 2^6$

$gcd(112, 64) = 2^4 = 16$

3) $\gcd(45, 0) = 45$

as $45 \mid 45$, $45 \mid 0$

45 is the Largest integer that divides 45

4) $10 = 2 * 5$, $21 = 3 * 7$

$\gcd(10, 21) = 1$

5) $17 = 17^1$, $22 = 2 * 11$

$\gcd(17, 22) = 1$

* Algorithm for div & mod

$q = \lfloor \frac{a}{d} \rfloor$, $r = a \bmod d$

algorithm Division (a, d)

$q = 0$

$r = |a|$

while $r >= d$ do

$r = r - d$

$q = q + 1$

if $a < 0$ then

if $r = 0$ then

$q = -q$

else

$r = d - r$

$q = -(q + 1)$

The run-time of the algorithm is $O(|q|)$

Taking encoding of integers into account, the run-time is $O(|q| \log |a|)$

Example:-

Find the quotient and remainder of dividing -11 by 3?

Sol:-

Using the algorithm

$|-11| = 11$

$11 \text{ div } 3 = 3$, $11 \bmod 3 = 2$

$-11 < 0$

$\therefore q = -(3+1) = -4$, $r = 3-2 = 1$

we can obtain the same result

using:

$$q = \lfloor \frac{a}{d} \rfloor \ \& \ r = a - q * d$$

$$q = \lfloor \frac{-11}{3} \rfloor = -4$$

$$r = -11 - (-4)(3) = 1$$

* Modular Exponentation

if we would like to get $b^n \bmod m$

where b^n is large

we use the identity

$$ab \bmod m = \left((a \bmod m)(b \bmod m) \right) \bmod$$

and get binary representation of

then apply the algorithm

algorithm modularExp(b, n=a[0 ... k-1], m)

binary representation of n

```
x = 1
Power = b mod m
for i = 0 to k-1 do
  if a[i] = 1 then
    x = (x * Power) mod m
  power = (Power * power) mod m
return x
```

The algorithm may be implemented to have run time $O((\log m)^2 \log n)$

Example:

Find $3^{11} \bmod 16$

Sol:

$11 = (1011)_2$

initially $x = 1$, Power $= 3 \bmod 16 = 3$

$i = 0$: $a_0 = 1$ $x = (1*3) \bmod 16 = 3$, Power $= (3^2) \bmod$

$i = 1$: $a_1 = 1$ $x = (3*9) \bmod 16 = 11$, Power $= (9^2) \bmod$

$i = 2$: $a_2 = 0$ $x = 11$, Power $= (1^2) \bmod 16 = 1$

$i = 3$: $a_3 = 1$ $x = (11*1) \bmod 16 = 11$

$3^{11} \bmod 16 = 11$

1011

Theorem :-

Let $a = qb + r$ where $a, q, b, r \in \mathbb{Z}$

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

Proof :-

1) Let $d \mid a$, $d \mid b$

$\therefore d \mid a - q * b$

$\therefore d \mid r$

$\therefore$ any common divisor of a, b is also

" " " b, r

2) Let $d \mid b$, $d \mid r$

$d \mid qb + r$

$d \mid a$

$\therefore$ any common divisor of b, r is

" " " a, b

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

* Euclidean algorithm :-

used to get $\gcd(a, b)$

algorithm EUCLID (a, b)

$x = a$

$y = b$

while $y \neq 0$ do

$r = x \bmod y$

$x = y$

$y = r$

return x

Complexity:-

In each iteration:

- the new value of x is the y_{old}
- " " " " y is $x_{old} \bmod y_{old}$ (r)

which is $\leq \frac{x_{old}}{2}$

because $r = x \bmod y$

if $y \leq x/2$ $r < x/2$

if $y > x/2$ $\rightarrow r = x - y$
$r < x/2$

So the original values of x, y are reduced by at least 1 half in every iteration

$\therefore$ run time of the algorithm is $O(\lceil \frac{a}{b} \rceil \log b)$ assuming $b \leq a$

Example:-

Find the GCD of 27 and 63?

Sol:-

$27 = 0 * 63 + 27$

$63 = 2 * 27 + 9$

$27 = 3 * 9 + 0$

Last non zero remainder

$\therefore \gcd(27, 63) = 9$

* GCD as a Linear Combinations

If $a, b \in \mathbb{Z}^+$ then

$\gcd(a, b) = sa + tb$

for $s, t \in \mathbb{Z}$

Example :-

Express gcd(252, 198) as a Linear Combinations of 252 and 198?

Sol:-

Using Euclid's algorithm to get gcd

$252 = 1 * 198 + 54$

$198 = 3 * 54 + 36$

$54 = 1 * 36 + 18$

$36 = 2 * 18 + 0$

$\gcd(252, 198) = 18$

Working backwards:

$18 = 54 - 1 * 36$

$= 54 - (198 - 3 * 54)$

$= 4 * 54 - 198$

$= 4[252 - 198] - 198$

$= 4 * 252 - 5 * 198$

$\therefore \gcd(252, 198) = 4 * 252 - 5 * 198$

Theorem:

If $a, b, c \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$ a

$a \mid bc$ then $a \mid c$

proof:

$\gcd(a, b) = sa + tb = 1$

multiply by c

$sac + tbc = c$

$a \mid sac$, $a \mid tbc$ [because $a \mid bc$

$\therefore a \mid sac + tbc$

$\therefore a \mid c$

Theorem:

If p is a prime & $p \mid a_1 a_2 \cdots a_n$ where $a_i \in \mathbb{Z}$ then

$p \mid a_i$ for some i

Uniquness of prime factorization

Proof:

Suppose that we have 2 prime factorization for n

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

removing all common factors of 2 factorizations we get:

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

$$p_{i_1} \mid p_{i_1} p_{i_2} \cdots p_{i_u}$$

$\therefore P_{i1} \mid q_{j1} q_{j2} \cdots q_{jv}$

from the pervions theorem

$\therefore P_{i1} \mid q_{jk}$ for some k

but P_{i1}, q_{jk} are primes

So P_{i1} can't divides q_{jk} [Contrad

$\therefore$ there exist a unique prime

factorization for any $n \in \mathbb{Z}$

Sec 4.3 : (7th Edition)

(11) Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x that can't be written as the ratio of 2 integers

Sol:-

by Contradication

assume $\log_2 3$ is rational

$\log_2 3 = \frac{a}{b}$ $(a, b \in \mathbb{Z}^+)$

$2^{\frac{a}{b}} = 3$

$\left(2^{\frac{a}{b}}\right)^b = 3^b$

$\therefore 2^a = 3^b$ [Contradication with the Fundamental theorem of arithmetic]

$\hookrightarrow$ prime factorization for each positive integer $\boxed{\text{is unique}}$

$\therefore \log_2 3$ is irrational

Remember:

Geometric sequence:

$a, ar, ar^2, \ldots$

Geometric series:-

$S = a + ar + ar^2 + \ldots$

finite

$S = a + ar + ar^2 + \ldots + ar^{n-1}$

$$\boxed{S = a\frac{1-r^n}{1-r}}$$

infinite

$S = a + ar + \ldots$

$|r| < 1$

$$\boxed{S = \frac{a}{1-r}}$$

$|r| \geq 1$

diverage

a/b

c/d

$b = am$
$d = cn$

$acmn$

Quiz 7.1 (Spring 2014):

prove or disprove

a) For $a, b, c, d \in \mathbb{Z}^+$, if $a|b$ and $c|d$, then $ac|bd$

Sol:-

$a|b \longrightarrow b = am \quad (m : int)$

$c|d \longrightarrow d = cn \quad (n : int)$

$b = ma$
$d = nc$
$bd = (mn)ac$
$(mn : int)$ $ac|bd$

$\therefore bd = ac\,mn$

$\therefore ac|bd$

b) For $c, d, n, m \in \mathbb{Z}^+$ with $n > 1$, if $mc \equiv md \pmod{n}$, then $c \equiv d \pmod{n}$?

$n|mc-md$

$n|c-d$

Sol:-

False, Counter example $m = 8$, $c = 3$, $d = 5$, $n = 4$

$mc = 24$, $md = 40$

$4|24-40$ $\quad 4|-16$

$4|3-5$ $\quad 4|2$

$4|2(3-1)$

$4|2(2)$ ✓

$4|2 \rightarrow ?$

$mc - md = -24$

$n \mid mc - md$

$\therefore (mc \equiv md) \bmod n$ but n does

divide $c - d$

Quiz 7.2 (Spring 2014):

Prove or disprove:

a) For $a, b, c, d \in \mathbb{Z}^+$, if $ac \mid bd$ then

$a \mid b$ and $c \mid d$

Sol:-

False, Counter example:

$a = 2, c = 3, b = 1, d = 6$

$ac \mid bd$ but a doesn't divide

$6 \mid 6$ ✓

$\overset{a}{3} \times \overset{c}{2} \mid \overset{b}{6} \times \overset{d}{1}$ ✓

b) For $c, d, n, m \in \mathbb{Z}^+$ with $n > 1$ 361

if $c \equiv d \pmod{n}$, then $mc \equiv md \pmod{n}$

Sol:-

$c \equiv d \bmod n$

$n \mid c-d$

$n \mid mc-md$?

$(c-d) = tn$

$mc-md = mnt$

n 8 4 2 1

$n \mid c-d$

$c-d = nt$ (t: int)

$mc - md = n\,mt$

mt is integer

then $\therefore n \mid mc-md$

$\therefore mc \equiv md \pmod{n}$

Quiz 7.1 (Fall 2014):

b Using the algorithm you learned in class, compute the value of

$7^{12} \bmod 13$

$12 = (1100)_2$

initially $x = 1$ Power $= 7 \bmod 13 =$

$i = 0$: $a_0 = 0$ $x = 1$, Power $= 7^2 \bmod 13 =$

$i = 1$: $a_1 = 0$ $x = 1$, Power $= 10^2 \bmod 13 =$

$i = 2$: $a_2 = 1$ $x = (1 * 9) \bmod 13 = 9$, Power $= 9^2 \bmod 13 =$

$i = 3$: $a_3 = 1$ $x = (9 * 3) \bmod 13 = 1$

$\therefore 7^{12} \bmod 13 = 1$

Quiz 7.2 (Fall 2014):

Using the algorithm you learned in the class, compute the value of

$7^9 \bmod 13$

8 4 2
8 4 2 1
1 0 0 1
1 1 0 0

Sol:-

$9 = (1001)_2$

initially $X = 1$, Power $= 7 \bmod 13 = 7$

$i=0$: $a_0 = 1$ $X = (1 * 7) \bmod 13 = 7$, Power $= 7^2 \bmod 13 = 10$

$i=1$: $a_1 = 0$ $X = 7$, Power $= 10^2 \bmod 13 = 9$

$i=2$: $a_2 = 0$ $X = 7$, Power $= 9^2 \bmod 13 = 3$

$i=3$: $a_3 = 1$ $X = (7 * 3) \bmod 13 = 8$

$\therefore 7^9 \bmod 13 = 8$

Quiz 8.1 (Spring 2015)

a) For $a_1, a_2, b_1, b_2 \in Z^+$, if $a_1 | 2a_2$ and $b_1 | 2b_2$ then $a_1 b_1 | 2a_2 b_2$

$2a_2 = m a_1$
$2b_2 = m b_1$

$4a_2b_2 = (mn) a_1 b_1$

Sol:-

$a_1 b_1 | 4a_2b_2$
$8 | n * 1$

$a_1 | 2a_2$

$2a_2 = m a_1$ (m int)

$b_1 | 2b_2$

$2b_2 = b_1 (n)$ (n : int)

$2a_2 = m a_1$ (m → int)
$2b_2 = n b_1$ (n → int)

Multiply the 2 equ:

$4 a_2 b_2 = a_1 b_1 (mn)$

$4a_2b_2 = mn\, a_1 b_1$

$2a_2b_2 = \frac{mn}{2} a_1 b_1$

$a_1 b_1 \mid 4a_2 b_2$

but $a_1 b_1$ may not divide $4a_2 b_2$

Counter example:

$a_1 = 2$, $a_2 = 1$, $b_1 = 2$, $b_2 = 1$

$a_1 \mid 2a_2$ & $b_1 \mid 2b_2$

but $a_1 b_1 = 4$, $2a_2 b_2 = 2$

$a_1 b_1$ doesn't divide $2a_2 b_2$

b) For $a, b, m \in \mathbb{Z}$, with $m \geq 2$, if $a \equiv b \pmod{m}$

then $a^2 \equiv b^2 \pmod{m}$

Sol:

$a \equiv b \pmod{m}$

$m \mid a-b$

$a - b = mn$ (n: int)

$(a-b)(a+b) = mn(a+b)$

$a^2 - b^2 = mn(a+b)$

$(a-b)(a+b)$

$a^2 - b^2 = (a+b)$

$m \mid a^2 - b^2$

$a^2 \equiv b^2 \bmod$

$a \equiv b \pmod{m}$

$m \mid a-b$

$(a-b)^2 = mn$

$(a-b)(a+b) = mn(a+b)$

$a^2 - b^2 = mn(a+b)$

$a^2 - 2ab + b^2 =$

$\therefore m \mid a^2 - b^2$

$\therefore a^2 \equiv b^2 \pmod{m}$

Quiz 7.1 (Fall 2015)

Let $a, b, c, d \in \mathbb{Z}^+$. If $a \mid b$ and $c \mid d$, then

$a^c \mid b^d$

Sol:-

$a \mid b$ $\quad b = am \quad (m : \text{int})$

$c \mid d$ $\quad d = cn \quad (n : \text{int})$

$b^d = (am)^{cn} = a^{cn} m^{cn}$

$= a^c \, a^{cn-c} \, m^{cn}$

$= a^c \times \text{int}$

$\therefore a^c \mid b^d$

$b = ma$

$d = nc$

$b^d = m^d a^d$

$= m^{nc} a^{nc}$

$= m^{nc} a^{c}$

$b = ma$ $\quad m \to \text{int}$

$d = nc$ $\quad \text{int}$

$m \mid a^2 - b^2$

$(a-b) = mn$

$(a-b)(a+b) = (a+b)mn$

$a^2 - b^2 = (a+b)mn$

$b^d = (ma)^d$

$d = nc$

$b^d = m^{nc} a^{nc}$

To calcul..

Quiz 8.1 (Spring 2016)

prove or disprove

If $a, b \in \mathbb{Z}^+$ and $\log_2 a \mid \log_2 b$ then $a \mid b$

Sol:-

Counter example: Let $a = 3$, $b = 1$

$\log_2 3 \mid \log_2 1$ but 3 doesn't div 1

$\log_2 1 \to 0$

$\therefore$ False

Quiz 8.2 (Spring 2016)

If $m, n \in \mathbb{Z}^+$ and $\ln m \mid \ln n$ then $m \mid n$

Sol:-

Counter example:

Let $m = 2$, $n = 1$

$\ln m \mid \ln n$ but 2 doesn't div 1

$\ln 1 = 0$

$\ln 2 \mid \ln 1$

$2 \mid 1$ ×

$\therefore$ False

Quiz 9.1 (Spring 2016)

Using the efficient modular exponentiation algorithm you learned in class, compute the value of $6^{10} \bmod 11$ 8 4 2 1

Show all your steps?

Sol:-

8 4 2 0
0 1 0

$10 = (1010)_2$

initially $x = 1$, Power $= 6 \bmod 11 = 6$

$i = 0$: $a_0 = 0$, $x = 1$, Power $= 6^2 \bmod 11 = \boxed{3}$

$i = 1$: $a_1 = 1$, $x = (1*3) \bmod 11 = 3$, Power $= 3^2 \bmod 11 = 9$

$i = 2$: $a_2 = 0$, $x = 3$, Power $= 9^2 \bmod 11 = 4$

$i = 3$: $a_3 = 1$, $x = (3*4) \bmod 11 = \boxed{1}$

$\boxed{6^{10} \bmod 11 = 1}$

Quiz 9.2 (Spring 2016)

Same Question for: $6^{12} \bmod 11$

Sol:- $(12)_2 = 1100$

initially $x = 1$, Power $= 6 \bmod 11 = 6$

$i = 0$: $a_0 = 0$, $x = 1$, Power $= 6^2 \bmod 11 = 3$

$i = 1$: $a_1 = 0$, $x = 1$, Power $= 3^2 \bmod 11 = 9$

$i = 2$: $a_2 = 1$, $x = (1*9) \bmod 11 = 9$, Power $= 9^2 \bmod 11 = 4$

$i = 3$: $a_3 = 1$, $x = (9*4) \bmod 11 = \boxed{3}$

$\boxed{6^{12} \bmod 11 = 3}$

Quiz 8.1 (Fall 2016)

Show that there is no $n \in \mathbb{Z}$ such that $n \equiv 3 \pmod 4$ and $n \equiv 5 \pmod 8$

Sol:-

y Contradication

assume that there exist $n \in \mathbb{Z}$ such that $n \equiv 3 \pmod 4$, $n \equiv 5 \pmod 8$

$4 \mid n-3$ $\qquad$ $8 \mid n-5$

$n-3 = 4k$ (k = int) $\qquad$ $n-5 = 8m$ (m:

$n = 4k+3$ $\qquad$ $n = 8m+5$

$\therefore$ $4k+3 = 8m+5$

$4k = 8m+2$

$n = 4m+3$
$n = 8k+5$

$k = 2m + \frac{1}{2}$

$4m+3 = 8k+5$

$k8$

$k =$

m is integer

$m = \frac{8k+2}{4}$

$m = 2k + \frac{1}{2}$

$k = 2m + \frac{1}{2}$ is not integer whi

make Contradication with k is in

$\therefore$ there exist no $n \in \mathbb{Z}$ such that

$n \equiv 3 \pmod 4$, $n \equiv 5 \pmod 8$

Quiz 8.2 (Fall 2016)

Show that there is no $n \in \mathbb{Z}$ such that

$n \equiv 2 \pmod 3$ and $n \equiv 4 \pmod 6$

$3 \mid n-2 \qquad n-2 = 3k$

$6 \mid n-4 \qquad n-4 = 6m$

$3k+2 = 6m+4$

$k = 2m + 2/3$ ✗

Sol :-

By Contradication

assume that there exist $n \in \mathbb{Z}$ such that

$n \equiv 2 \pmod 3$, $n \equiv 4 \pmod 6$

$3 \mid n-2$, $6 \mid n-4$

$n-2 = 3k$ (k int) , $n-4 = 6m$ (m int)

$n = 3k+2$, $n = 6m+4$

$\therefore 3k+2 = 6m+4$

$k = 6m+2$

$k = 2m + 2/3$

$3 \mid n-2$

$6 \mid n-4$

$n-2 = 3k$ $\boxed{n = 3k+2}$

$n-4 = 6m$ $\boxed{n = 6m+4}$

$3k+2 = 6m+4$

$3k = 6m+2$

$k = \frac{6m+2}{3}$

m is integer

$k = 2m + 2/3$ not integer which make Contradication with k integer

$\therefore$ there exist no $n \in \mathbb{Z}$ such that $n \equiv 2 \pmod 3$, $n \equiv 4 \pmod 6$

Quiz 9.1 (Fall 2016)

Use the methodology presented in class to represent gcd(254, 103) as a linear combination of 254 and 103. Show all your steps?

Sol:-

$254 = 2 * 103 + 48$

$103 = 2 * 48 + 7$

$48 = 6 * 7 + 6$

$7 = 1 * 6 + 1$

$6 = 6 * 1 + 0$

$\gcd(254, 103) = 1$

working backwards:

$1 = 7 - 1 * 6$

$1 = 7 - 1 * [48 - 6 * 7]$

$1 = 7 * 7 - 48$

$1 = 7 * (103 - 2 * 48) - 48$

$1 = 7 * 103 - 15 * 48$

$1 = 7 * 103 - 15 (254 - 2 * 103)$

$1 = 37 * 103 - 15 * 254$

$\gcd(254, 103) = -15 * 254 + 37 * 103$

Quiz 9.2 (Fall 2016)

Same Question in 9.1

Sol:-

$255 = 2 * 106 + 43$

$106 = 2 * 43 + 20$

$43 = 2 * 20 + 3$

$20 = 6 * 3 + 2$

$3 = 1 * 2 + 1$

$2 = 2 * 1 + 0$

$\Rightarrow \gcd(255, 106) = 1$

Working backwards:

$1 = 3 - 1 * 2$

$1 = 3 - 1 * (20 - 6 * 3)$

$1 = 7 * 3 - 1 * 20$

$1 = 7 * (43 - 2 * 20) - 1 * 20$

$1 = 7 * 43 - 15 * 20$

$1 = 7 * 43 - 15 [106 - 2 * 43]$

$1 = 37 * 43 - 15 * 106$

$1 = 37 * [255 - 2 * 106] - 15 * 106$

$1 = 37 * 255 - 89 * 106$

$\rightarrow \gcd(255, 106)$

$\gcd(255, 106)$

$255 = 106 * 2 + 43$

$106 = 43 * 2 + 20$

$43 = 20 * 2 + 3$

$20 = 3 * 6 + 2$

$3 = 2 * 1 + \boxed{1}$

$2 = 2 * 1 + 0$

$1 = 3 - 2 * 1$

$1 = 3 - (20 - 3 * 6) * 1$

$1 = 3 * 7 - 20 * 1$

$1 = (43 - 20 * 2) * 7 - 20 * 1$

$1 = 43 * 7 - 20 * 15$

$1 = 43 * 7 - (106 - 43 * 2) * 15$

$1 = 43 * 37 - 106 * 15$

$1 = [255 - 2 * 106] * 37 -$

$1 = 255 * 37 - 89 * 106$

Assignment 9

Sec 3.4:

6. Show that if a, b, c, and d are integers such that a | c and b|d, then a b | cd.

Solution:-
a | c so c = a * n (n is integer)
b | d so d = b * m (m is integer)

cd = ab * nm
a b | cd

8. Prove or disprove that if a | bc, where a, b, and c are positive integers, then a| b or a |c.

Solution:-
Let a=6 , b= 3 , c=4
a | b c but a ∤ b and a ∤ c
so if a | bc, where a, b, and c are positive integers, w can't conclude a| b or a |c.

10. What are the quotient and remainder when
a) 44 is divided by 8?
b) 777 is divided by 21 ?
c) -123 is divided by 19?
d) -1 is divided by 23?
e) -2002 is divided by 87?
f) 0 is divided by 17?
g) 1,234,567 is divided by 1001?
h) -100 is divided by 101?

Solution:-

a) $q = \left\lfloor \frac{a}{d} \right\rfloor = \left\lfloor \frac{44}{8} \right\rfloor = 5$, $r = a \bmod d = a - q * d = 44 - 5 * 8 = 4$

b) $q = \left\lfloor \frac{a}{d} \right\rfloor = \left\lfloor \frac{777}{21} \right\rfloor = 5$, $r = a \bmod d = a - q * d = 44 - 5 * 8 = 4$

c) $|a| = 123$

$q = \left\lfloor \frac{|a|}{d} \right\rfloor = \left\lfloor \frac{123}{19} \right\rfloor = 6$, $r = |a| - q * d = 123 - 6 * 19 = 9$

$q = -(q+1) = -7$, $r = d - r = 19 - 9 = 10$

d) $q = -1, r = 22$
e) $q = -24, r = 86$
f) $q = 0, r = 0$
g) $q = 1233, r = 334$
h) $q = -1, r = 1$

22. Show that if a, b, c, and m are integers such that m > 2, c > 0, and a ≡ b (mod m), then ac ≡ bc (mod mc)?

Solution:-

$a \equiv b \ (mod\ m)$

$m | a - b$

$a - b = m * n \quad (n \text{ is integer})$

$ac - bc = mc * n$

$mc | ac - bc$

$ac \equiv bc \ (mod\ mc)$

23. Find counterexamples to each of these statements about congruences.

a) If ac ≡ bc (mod m), where a, b, c, and m are integers with m ≥ 2, then a ≡ b (mod m).

b) If a ≡ b (mod m) and c ≡ d (mod m), where a, b, c, d, and m are integers with c and d positive and m > 2, then a ≡ b (mod m).

Solution:-

a) m = 2, c = 2, a = 0, and b = 1.

b) m = 5, a = 3, b = 3, c = 1, d = 6.

24. Prove that if n is an odd positive integer, then $n^2 \equiv 1$ (mod 8).

Solution:-

n is odd

$n = 2k + 1 \quad (k \text{ is an integer})$

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

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

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

$n^2 - 1 = 4k(k + 1)$

If k is even $k = 2m$ (k is an integer)

$k(k + 1) = 2m(2m + 1)$ which is even

If k is odd $k = 2m + 1$ (k is an integer)

$k(k + 1) = (2m + 1)(2m + 2) = (m + 1)(2m + 1)$ which is even

$k(k + 1)$ is even

$k(k + 1) = 2t$ (t is an integer)

$n^2 - 1 = 8t$

$\frac{(n^2-1)}{8} = t$

8 divides $n^2 - 1$

$n^2 \equiv 1$ (mod 8)

Sec 3.5:

2. Determine whether each of these integers is prime.

a) 19 b) 27
c) 93 d) 101
e) 107 f) 113

Solution:-

a) $\sqrt{19} = 4.3589$

Prime numbers less than $\sqrt{19}$ are 2, 3

$\frac{19}{2} = 9.5$ (not integer)

$\frac{19}{3} = 6.333$ (not integer)

So 19 is a prime number

b) $\sqrt{27} = 5.1962$

Prime numbers less than $\sqrt{27}$ are 2, 3, 5

$\frac{27}{2} = 13.5$ (not integer)

$\frac{27}{3} = 9$ (integer)

So 19 is not prime number

c) $\sqrt{93} = 9.6437$

Prime numbers less than $\sqrt{93}$ are 2, 3, 5, 7

$\frac{93}{2} = 46.5$ (not integer)

$\frac{93}{3} = 31$ (integer)

So 93 is not prime number

d) $\sqrt{101} = 10.0499$

Prime numbers less than $\sqrt{101}$ are 2, 3, 5, 7

$\frac{101}{2} = 50.5$ (not integer)

$\frac{101}{3} = 33.6667$ (not integer)

$\frac{101}{5} = 20.2$ (not integer)

$\frac{101}{7} = 14.4286$ (not integer)

So 101 is prime number

e) 107 is prime f) 113 is prime

4. Find the prime factorization of each of these integers.

a) 39 b) 81 c) 101
d) 143 e) 289 f) 899

Solution:-

a) $\frac{39}{2} = 19.5$ (not integer)

$\frac{39}{3} = 13$

$\frac{13}{3} = 4.33$ (not integer)

$\frac{13}{5} = 2.6$ (not integer)

$\frac{13}{7} = 1.8571$ (not integer)

$\frac{13}{11} = 1.1818$ (not integer)

$\frac{13}{13} = 1$

$39 = 3*13$

b) $\frac{81}{2} = 40.5$ (not integer)

$\frac{81}{3} = 27$

$\frac{27}{3} = 9$

$\frac{9}{3} = 3$

$\frac{3}{3} = 1$

$81 = 3^4$

c) $101 = 101^1$
d) $143 = 11*13$
e) $289 = 17^2$
f) $889 = 29*31$

*6. How many zeros are there at the end of 100! ?

Solution:-

Zeros resulted from multiplying 2 by 5, so we need to get the greatest factor of 100! which is power of 2 (2^n)and greatest factor of 100! which is power of 5 (5^m)

$100! = 1*2*3*4*5*....*99*100$

The numbers which are divisible by 5 :
5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100

$5 = 5^1$
$10 = 2*5^1$
$15 = 3*5^1$
$20 = 2^2*5^1$
$25 = 5^2$
$30 = 2*3*5^1$
$35 = 7*5^1$
$40 = 2^3*5^1$
$45 = 3^2*5^1$
$50 = 2*5^2$
$55 = 11*5^1$
$60 = 2^2*3*5^1$
$65 = 13*5^1$
$70 = 2*7*5^1$
$75 = 3*5^2$
$80 = 2^4*5$
$85 = 17*5^1$
$90 = 2*3^2*5^1$
$95 = 19*5^1$
$100 = 2^2*5^2$

The greatest common divisor of 100! Which is multiple of 5 is
$5^1*5^1*5^1*5^1*5^2 * 5^1*5^1*5^1*5^1*5^2 * 5^1*5^1*5^1*5^1*5^2 * 5^1*5^1*5^1*5^1*5^2 = (5^1*5^1*5^1*5^1*5^2)^4 = 5^{24}$

The numbers which are divisible by 2 : all even number (50 numbers) so The greatest common divisor of 100! Which is multiple of $2 \geq 2^{50}$

So the greatest common divisor of 100! Which is multiple of 10 is $(2*5)^{24}$

So there are 24 zeros at the end of 100!

8. Prove that for every positive integer n, there are n consecutive composite integers. [Hint: Consider the n consecutive integers starting with $(n + 1)! + 2$.]

Solution:-
$(n + 1)! + 2 = 1*2*3*4*.....*(n+1) +2$
$(n + 1)! + 2 = 2* (1*3*4*.....*(n+1) +1)$

$2 \mid (n + 1)! + 2$ so $(n + 1)! + 2$ is composite

$(n + 1)! + 3 = 1*2*3*4*.....*(n+1) +3$

$(n+1)! + 3 = 3 * (1*2*4*5 \ldots\ldots *(n+1) + 1)$

$3 \mid (n+1)! + 3$ so $(n+1)! + 3$ is composite

Similarly for any integer i ($2 \leq i \leq n+1$)

$i \mid (n+1)! + i$ so $(n+1)! + i$ is composite

so we have ($n+1-2+1 = n$) consecutive composite integers.

11. Which positive integers less than 30 are relatively prime to 30?

Solution:-

Each integer i that satisfy gcd(30,i) =1 is relatively prime to 30 so positive integers less than 30 which are relatively prime to 30 are :
1, 7, 11, 13, 17, 19, 23, 29

12. Determine whether the integers in each of these sets are pairwise relatively prime.
a) 21,34,55
b) 14,17,85
c) 25,41,49,64
d) 17,18, 19, 23

Solution -
a) 21=3*7 , 34=2*17 , 55=5*11
gcd (21,34) =1, gcd (21,55) =1 , gcd (34,55) =1
so the set is pairwise relatively prime
b) 14=2*7 , 17=17[1] , 85=5*17
gcd (14,17) =1 , gcd (14,85) =1 , gcd (17,85) =17
so 17,85 are not pairwise relatively prime
so the set is not pairwise relatively prime

c) The set is pairwise relatively prime
d) The set is pairwise relatively prime

14. We call a positive integer perfect if it equals the sum of its positive divisors other than itself.
a) Show that 6 and 28 are perfect.
b) Show that $2^{P-1}(2^P - 1)$ is a perfect number when $2^P - 1$ is prime.

Solution:-
a) Divisors of 6: 1, 2, 3, 6

Divisors of 6 other than 6 : 1, 2, 3

$1+2+3 = 6$

So 6 is perfect integer

Divisors of 28: 1, 2, 4, 7 , 14, 28

Divisors of 28 other than 28 : 1, 2, 4, 7 , 14

$1+2+4+7+14 = 28$

So 28 is perfect integer

b) Divisors of $2^{P-1}(2^P - 1)$ other than itself:

$1, 2, 4, \ldots, 2^{P-1}, (2^P - 1), 2*(2^P - 1), 4*(2^P - 1), \ldots\ldots, 2^{P-2}*(2^P - 1)$

$1+2+4+\ldots+2^{P-1}+(2^P - 1)+2*(2^P - 1)+4*(2^P - 1)+\ldots\ldots+2^{P-2}*(2^P - 1)=$

$1\frac{1-2^p}{1-2}+(2^p-1)\frac{1-2^{p-1}}{1-2}=$

$-1+2^p+(2^p-1)*(-1+2^{p-1})=$

$-1+2^p+-2^p+1+2^{2p-1}-2^{p-1}=$

$2^{2p-1}-2^{p-1}= 2^{p-1}(2^p-1)$

So $2^{p-1}(2^p-1)$ is perfect integer

[Sum of geometric a, ar, ar², ar³, ... ar^{n-1}]

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

20. What are the greatest common divisors of these pairs of integers?

a) $2^2.3^3.5^5,\ 2^5.3^3.5^2$

b) $2.3.5.7.11.13,\ 2^{11}.3^9.11.17^{14}$

c) $17, 17^{17}$

d) $2^2.7,\ 5^3.13$

e) 0, 5

f) 2. 3 . 5 . 7, 2. 3 . 5 . 7

Solution:-

a) $\gcd(2^2.3^3.5^5,\ 2^5.3^3.5^2) = 2^{\min(2,5)}.3^{\min(3,3)}.5^{\min(5,2)} = 2^2.3^3.5^2$

b) $\gcd(2.3.5.7.11.13,\ 2^{11}.3^9.11.17^{14}) = 2*3*11$

c) $\gcd(17, 17^{17}) = 17$

d) $\gcd(2^2 . 7,\ 5^3 . 13) = 1$
e) $\gcd(0, 5) = 5$
f) $\gcd(2 . 3 . 5 . 7,\ 2 . 3 . 5 . 7) = 2 . 3 . 5 . 7$

24. Find gcd(1000, 625) and lcm(1000, 625) and verify that gcd(1000, 625) . lcm(1000, 625) = 1000 . 625?

Solution:-
$\frac{1000}{2} = 500$
$\frac{500}{2} = 250$
$\frac{250}{2} = 125$
$\frac{125}{5} = 25$
$\frac{25}{5} = 5$
$\frac{5}{5} = 1$
$1000=2^3 5^3$

$\frac{625}{5} = 125$
$\frac{125}{5} = 25$
$\frac{25}{5} = 5$
$\frac{5}{5} = 1$
$625=5^4$
$\gcd(1000,625)=5^3$

32. Show that if a, b, and m are integers such that m > 2 and a ≡ b (mod m), then gcd(a, m) = gcd(b, m).

Solution:-
a ≡ b (mod m)
a-b = m n (n is integer)
a = b + m n
any common divisor of (b , m) also divides a
b = a-mn
any common divisor of (a , m) also divides b
so the set of common divisors of (a , m) is the same set of common divisors of (b , m)

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

Sec 3.6:

20. Use Algorithm 5 to find 11^{644} mod 645.

Solution:-

$644 = (1010000100)_2$

Initially, x = 1 and power = 11 mod 645 = 11

$i = 0$: $a_0 = 0$, x = 1 and power = 11^2 mod 645 = 121 mod 645 = 121

$i = 1$: $a_1 = 0$, x = 1 and power = 121^2 mod 645 = 14641 mod 645 = 451

$i = 2$: $a_2 = 1$, x = (1*451) mod 645 = 451 and power = 451^2 mod 645 = 203401 mod 645 = 226

$i = 3$: $a_3 = 0$, x = 451 and power = 226^2 mod 645 = 51076 mod 645 = 121

$i = 4$: $a_4 = 0$, x = 451 and power = 121^2 mod 645 = 14641 mod 645 = 451

$i = 5$: $a_5 = 0$, x = 451 and power = 451^2 mod 645 = 203401 mod 645 = 226

$i = 6$: $a_6 = 0$, x = 451 and power = 226^2 mod 645 = 51076 mod 645 = 121

$i = 7$: $a_7 = 1$, x = (451*121) mod 645 = 391 and power = 121^2 mod 645 = 14641 mod 645 = 451

$i = 8$: $a_8 = 0$, x = 391 and power = 451^2 mod 645 = 203401 mod 645 = 226

$i = 9$: $a_9 = 1$, x = (391*226) mod 645 = 1.

11^{1001} mod 645=1

22. Use Algorithm 5 to find 123^{1001} mod 101?

Solution:-

$1001 = (1111101001)_2$

Initially, x = 1 and power = 123 mod 101 = 22

$i = 0$: $a_0 = 1$, x = (1*22) mod 101 = 22 and power = 22^2 mod 101= 484 mod 101 = 80

$i = 1$: $a_1 = 0$, x = 22 and power = 80^2 mod 101= 6400 mod 101= 37

$i = 2$: $a_2 = 0$, x = 22 and power = 37^2 mod 101= 1369 mod 101= 56

$i = 3$: $a_3 = 1$, x = (22*56) mod 101 =1232 mod 101=20 and power = 56^2 mod 101= 5

$i = 4$: $a_4 = 0$, x = 20 and power = 5^2 mod 101= 25 mod 101= 25

$i = 5$: $a_5 = 1$, $x = (20*25) \bmod 101 = 96$ and power $= 25^2 \bmod 101 = 19$

$i = 6$: $a_6 = 1$, $x = (96*19) \bmod 101 = 6$ and power $= 19^2 \bmod 101 = 58$

$i = 7$: $a_7 = 1$, $x = (6*58) \bmod 101 = 45$ and power $= 58^2 \bmod 101 = 31$

$i = 8$: $a_8 = 0$, $x = 45$ and power $= 31^2 \bmod 101 = 52$

$i = 9$: $a_9 = 1$, $x = (45*52) \bmod 101 = 17$,

$123^{1001} \bmod 101 = 17$

24. Use the Euclidean algorithm to find

a) gcd(1,5).
b) gcd(100, 101).
c) gcd(123,277).
d) gcd(1529, 14039).
e) gcd(1529,14038).
f) gcd(11111,111111).

Solution:-

a) 1=0*5+1
5=5*1+0
gcd(1,5)=1

b) 100=0*101+100
101=1*100+1
100=100*1+0
gcd(101,100)=1

c) 123=0*277+123
277=2*123+31
123=3*31+30
31= 1*30+1
30=30*1+0
gcd(123,277)=1

d) 1529 = 0*14039+1529
14039 = 9*1529+278
1529 = 5*278 +139
278=2*139+0
gcd(1529, 14039)=139

e) gcd(1529,14038)= 1

f) gcd(11111,111111)=1

Sec 3.6:

2. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 9,11
b) 33,44
c) 35,78
d) 21, 55
e) 101, 203
f) 124, 323
g) 2002,2339
h) 3457,4669
i) 10001, 13422

Solution:-

a) Euclidean algorithm to get gcd (9,11)

9 = 0*11+9
11=1*9+2
9 = 4*2+1
2 = 2*1+0
gcd(9,11)=1

working backward
1= 9-4*2
1= 9- 4* (11-9)
1= 9 – 4*11 + 4*9
1= 5*9 – 4*11
gcd(9,11)= 5*9 – 4*11

a) Euclidean algorithm to get gcd (33,44)

33 = 0*44+33
44 = 1*33+11
33 = 3*11 + 0
gcd(33,44)=11

working backward
11= 44-1*33
gcd(33,44)= 44-1*33

b) Euclidean algorithm to get gcd (35,78)

35 = 0*78+35
78 = 2*35+8
35 = 4*8 +3
8 = 2*3+2
3 = 1*2+1

2 = 2*1+0

gcd(35,78)=1

working backward

1 = 3-1*2

1 = 3-1* (8 -2*3)

1 = 3*3 -1*8

1 = 3* (35-4*8) -8

1 = 3*35 -12*8-8

1=3*35-13*8

1=3*35-13*(78-2*35)

1=3*35-13*78+26*35

1=29*35-13*78

gcd(35,78)= 29*35-13*78

c) Euclidean algorithm to get gcd (21,55)

21 = 0*55+21

55 = 2*21+ 13

21 = 1*13 +8

13 = 1*8 +5

8 = 1*5 +3

5 = 1*3 +2

3 = 1*2 +1

2 =2*1 +0

gcd(21,55)= 1

working backward

1 = 3 -1*2

1 = 3 - (5-3)

1 = 2*3 – 5

1 = 2*(8-1*5) -5

1 = 2*8 -2*5-5

1 = 2*8-3*5

1 = 2*8 -3*(13-1*8)

1 = 5*8 -3*13

1 = 5*(21-13)-3*13

1 = 5*21 - 8*13

1 = 5*21 – 8*(55-2*21)

1 = 21*21 – 8*55

gcd(21,55) = 21*21 – 8*55

d) Euclidean algorithm to get gcd (21,55)

101 = 0*203+101
203 = 2*101 +1
101 = 101*1+0
gcd(101,203) = 1

working backward
1 = 203 – 2*101
gcd(101,203) =203 – 2*101

*13. Show that if m is a positive integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \bmod m/\gcd(c, m)$.

Solution:-

$ac \equiv bc \pmod{m}$

$ac - bc = m\,n$ (where n is an integer)

$c\,(a - b) = m\,n$

$\frac{c\,(a-b)}{m} = n$

$\gcd(c, m)$ divides both c, m

So $c = \gcd(c, m)\,k_1$ and $m = \gcd(c, m)\,k_2$ for some integers (k_1 and k_2)

$$\frac{\gcd(c,m)\,k_1(a-b)}{\gcd(c,m)\,k_2} = n$$

$$(a-b) = \frac{n\,k_2}{k_1}$$

$$(a-b) = \frac{n\,m}{k_1\,\gcd(c,m)}$$

$$k_1(a-b) = \frac{n\,m}{\gcd(c,m)}$$

$\frac{m}{\gcd(c,m)}$ divides $k_1(a-b)$ and $\gcd\left(\frac{m}{\gcd(c,m)}, k_1\right) = 1$

$\frac{m}{\gcd(c,m)}$ divides $(a-b)$

$$a \equiv b \bmod \frac{m}{\gcd(c,m)}$$