(14)

Represent

$$6 = ax + by$$

$$6 = 24 - 18$$

$$= 24 - (138 - 5 \cdot 24)$$

$$= 6 \cdot 24 - 138$$

$$= 6(162 - 138) - 138$$

$$= 6 \cdot 162 - 7 \cdot 138$$

$$= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162)$$

$$= 132 \cdot 162 - 7 \cdot 3054$$

$$= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054$$

$$= 132 \cdot 12378 + (-535) \cdot 3054$$

$$= 12378x + 3054y$$

$x = 132$

$y = -535$

This representation is not unique

$$6 = 3186 \cdot 12378 + (-12913) \cdot 3054$$

(15)

Least Common Multiple: The l.c.m m of two non-zero integers a and b, denoted by lcm (a,b) is the positive integer m satisfying the following :

(a) $a|m$ and $b|m$

(b) If $a|c$ & $b|c$ with $c>0$

then $m \leq c$.

Theorem: For positive integers a and b

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

Hint: $d = \gcd(a,b)$

$a = dr$, $b = ds$

If $m = \frac{ab}{d}$ then $m = as = rb$

$\Rightarrow a|m$ & $b|m$

Let $c|a$ & $c|b$

$c = au = bv$ for $u, v \in \mathbb{Z}$

$d = (a,b) \Rightarrow \exists\ x, y \in \mathbb{Z}$ s.t $d = ax+by$

(16)

$$\frac{c}{m} = \frac{cd}{ab}$$

$$= \frac{c}{ab}(ax + by)$$

$$= \frac{c}{b}x + \frac{c}{a}y$$

$$= vx + uy$$

$$\Rightarrow \quad m \leq c \quad \Rightarrow \quad m = l.c.m(a,b)$$

(17)

Diophantine Equation:

→Linear Diophantine Equation in One Variable is $ax = b$; $a, b \in \mathbb{Z}$, $x \in \mathbb{Z}$ $\left(= \frac{b}{a}\right)$

→Linear Diophantine Equation in two variable is of the form

$$ax + by = c;$$

$a, b, c \in \mathbb{Z}$, $a \neq b$ not zero

Theorem: The Linear Diophantine Equation $ax + by = c$ has a solution iff $d \mid c$ where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \frac{b}{d}t$$

$$y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}$$

(18)

Proof: Assume that x_0, y_0 is a solution of $ax + by = c$ and $d = (a,b)$.

To prove: $d \mid c$

As $d = (a,b) \Rightarrow$ $a = dr$

$\&$ $b = ds$

for some $r, s \in \mathbb{Z}$

Also $ax_0 + by_0 = c$

$\Rightarrow c = drx_0 + dsy_0 = d(rx_0 + sy_0)$

$\Rightarrow d \mid c$

Conversely: $d \mid c \Rightarrow c = dt$ for some $t \in \mathbb{Z}$

$d = (a,b) \Rightarrow \exists$ integers x_0 and y_0

such that $d = ax_0 + by_0$

$\therefore c = (ax_0 + by_0)t$

$= a(tx_0) + b(ty_0)$

Hence $ax + by = c$ has tx_0, ty_0 as a particular solution.

(19)

Let x', y' be any other solution,

then $ax_0 + by_0 = c = ax' + by'$

$\equiv a(x' - x_0) = b(y_0 - y') \quad - (1)$

$\gcd(a,b) = d \Rightarrow \exists\ r, s \in \mathbb{Z}$, $(r,s) = 1$

such that $a = dr$

$b = ds$

Equation (1) becomes

$r(x' - x_0) = s(y_0 - y')$

$r \mid s(y_0 - y')$ with $(r,s) = 1$

By Euclid's Lemma $r \mid y_0 - y'$

$\Rightarrow y_0 - y' = rt$ for some $t \in \mathbb{Z}$

$x' - x_0 = st$

$x' = x_0 + st = x_0 + \frac{b}{d}t$

$y' = y_0 - rt = y_0 - \frac{a}{d}t$

$ax' + by' = c$

Thus there are infinite number of solutions of the given equation, one for each value of t.

(20)

Example:

Solve

$$172x + 20y = 1000$$

$\gcd(172, 20) = ?$ (Euclidean Algo)

$$172 = 8 \cdot 20 + 12$$

$$20 = 1 \cdot 12 + 8$$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4$$

$\gcd(172, 20) = 4$ & $4 \mid 1000$

$\Rightarrow$ solution exists.

Express 4 as a Lineae Combination of 172 and 20.

$$4 = 12 - 1 \cdot 8 = 12 - (20 - 1 \cdot 12)$$
$$= 2 \cdot 12 - 20$$
$$= 2(172 - 8 \cdot 20) - 20$$
$$= 2 \cdot 172 + (-17) \cdot 20 \quad \text{— (1)}$$

Multiply (1) by ~~500~~ 250

$\Rightarrow$ $1000 = 500 * 172 + (-4250) * 20$

$x_0 = 500, \quad y_0 = -4250$

$x = x_0 + \frac{b}{d}t = 500 + 5t \qquad t \in Z$

$y = y_0 - \frac{a}{d}t = -4250 - 43t$

(21)

Congruence:

Def: Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbalized by

$$a \equiv b \pmod{n}$$

if n divides the difference $a-b$,

i.e, $a-b = kn$ for some $k \in \mathbb{Z}$.

e.g $3 \equiv 24 \pmod{7}$

$$-31 \equiv 11 \pmod{7}$$

→ If $n \nmid a-b$, we say a is incongruent to b modulo n and written as $a \not\equiv b \pmod{n}$.

→ Given a, Let q and r be its quotient and remainder upon division by n, i.e $a = qn + r$, $0 \le r < n$

$$\therefore a \equiv r \pmod{n}$$

(22)

→ r is residue or remainder of a congruence.

→ There are n choices of r, every integer is congruent modulo n to exactly one of the values 0, 1, 2, ... n-1. In particular

$a \equiv 0 \pmod{n}$ iff $n \mid a$.

→ The set of n integers 0, 1, 2, ... n-1 is called the set of least non-negative residue modulo n.

Theorem: For arbitrary integers a and b, $a \equiv b \pmod{n}$ iff a and b leave the same non-negative remainder upon division by n.

(23)

Proof: Suppose $a \equiv b \pmod{n}$

$\Rightarrow a = b + kn$ for some $k \in \mathbb{Z}$

& $b = qn + r$ for some

(By Division algorithm to b and n)

$\therefore a = qn + r + kn = (q+k)n + r$

$\Rightarrow$ a and b leaves the same remainder r.

Conversely: a and b leave the same remainder upon dividing by n.

$a = q_1 n + r$

& $b = q_2 n + r$

$\Rightarrow a - b = (q_1 - q_2) n$

$\Rightarrow a \equiv b \pmod{n}$

(24)

Theorem: Let $n>1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod{n}$

(b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$

(e) If $a \equiv b \pmod{n}$ then $a+c \equiv b+c \pmod{n}$ and $ac \equiv bc \pmod{n}$

(f) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for any positive integer k.