Assignment 1

z5304998

October 2020

Problem 1

(a):

Because $x, y \in Z, so\, that\, S_{2,-4} = \{2m - 4n : m, n \in Z\}$.
$When\ (m, n)\ are\ (0, 1), (1, 0), (0, 0), (2, 0), (0, 2)$
$S_{2,-4} = \{-4, 2, 0, 4, -8\}$

(*b*) :

$Because\ x, y \in Z, so\ that\ S_{12,18} = \{12m + 18n : m, n \in Z\}$
$when\ (m, n)\ are\ (0, 0), (1, 0), (0, 1), (1, -1), (-1, 1)$
$S_{12,18} = \{0, 12, 18, -6, 6\}$

(*c–i*):

$From\ d\ =\ gcd(x, y)\ We\ have\ d|x\ and\ d|y.\ So\ that,\ for\ m, n\ we\ have\ d|(mx+ ny) \in Z$
$So\ d|x\ and\ x \in dZ\ there\ fore\ S_{x,y} \subseteq \{n : n \in Z\ and\ d|n\}$

(*c − ii*):

$Because\ z \in S_{x,y}.\ from\ above\ question\ we\ have\ z \in dZ\ which\ is\ d|z.$
$Because\ z\ is\ smallest\ positve\ number,\ \ and\ d = gcd(x, y)\ we\ have\ d\ and\ z\ are\ positive.\ d > 0\ and\ z > 0$
$So\ z \leq d$

(*d − i*) :

$Because\ z|x\ ,\ z|y\ and\ z \in S, so\ that\ z = mx + ny : m, n \in Z\ and\ x\%z\ = 0,\ y\%z\ = 0$
$let\ z|g\ and\ g = kz\ for\ some\ k \in Z$
$g = (km)x + (kn)y : g \in S_{x,y}\, , S \in [0, z)$
$so\ that\ g \in [0, z).$
$Because\ z\ is\ smallest\ positve\ integer\ and\ g \in [0, z)$
$g\ =\ 0\ which\ is\ x\%z\ and\ y\%z\ = 0$
$which\ means\ z|x\ and\ z|y$
$(d - ii)\ From\ above, z|x, z|y\ .\ so\ z\ is\ common\ divisor\ of\ x\ and\ y.$
$Since\ d\ is\ the\ gcd.\ so\ z \leq d.$

Problem2

(*a*) :

$From\ wx = 1(mod\ y), gives\ y|wx - 1$
$From\ gcd(x, y) = 1\ and\ w[0, y)\ N\ gives\ integer\ w, w = d\%y : w \in [0, y)\ and\ d \in Z$

$From\ bezoul's\ identy\ gives\ \exists\ m, n \in Z\ for\ mx + ny = 1.\ And\ mx = 1(mod\ y)$

$let\ m = qy + w, q = \left\lfloor \frac{m}{y} \right\rfloor$
$So\ that:$
$(qy + w)x\ +\ ny = 1$
$qyx\ +\ wx\ + ny\ = 1$
$wx + (qx + n)y\ = 1$
$wx - 1 = -(qx + n)y$
$y|wx - 1, which\ s\ wx = 1(mod\ y)$

(b)
$Since\ y|kx, gives\ \exists a \in Z, kx = ry$
$Since\ gcd(x, y)\ = 1\ gives\ mx + ny\ = 1$
$mx + ny\ =\ 1$
$mxk + nyk\ =\ K$
$mry + nyk =\ k\ \ replace\ kx\ by\ ry$
$(rm + kn)y = k$
$so\ that\ y|k$
(c)
$let\ 2 integers\ w_1\ and\ w_2 \in\ [0, y) \cap N\ and\ w_1x = 1(mod\ y)\ w_2x = 1(mod\ y)$
$$Since\ \begin{cases} y|w_1x - 1 \\ y|w_2x - 1 \end{cases} gives \begin{cases} iy = w_1x - 1 \\ jy = w_1x - 1 \end{cases} where\ i\ and\ j\ \in Z$$
$so\ that\ w_1x - iy\ =\ w_2x - jy$
$(w_1 - w_2)x =\ (a - b)y$
$y|(w_1 - w_2)x.\ and\ because\ y|kx,\ gcd(x, y) = 1$
$so\ that\ y|w_1 - w_2$
$Since\ w_1\ w_2 \in [0, y)$
$w_1 - w_2\ =\ ky \in (-y, y)$
$w_1 - w_2 = 0$
$So\ that\ w_1\ equal\ to\ w_2,\ means\ only\ one\ w$
$exit$
Problem 3
$$\text{let} \begin{cases} a = m\%n,\ a \in [0, n) \\ m = \left\lfloor \frac{m}{n} \right\rfloor n + a, \quad \left\lfloor \frac{m}{n} \right\rfloor \geqslant 1 \end{cases}$$
$if\ \frac{3}{2}(n + (m\%n))\ <\ m +\ n\ exist$
$3(n + a) < 2m + 2n$
$3n + 3a < 2m + 2n$
$n + 3a\ < 2m$
$n + 3a <\ 2 \left\lfloor \frac{m}{n} \right\rfloor\ n + 2r$
$n + r < 2n \left\lfloor \frac{m}{n} \right\rfloor$
$left\ of\ eqution :\in [n, 2n)$
$right\ of\ eqution\ \in [2n, +\infty)$
$left\ \ < right\ exist$