amssymb

assignment1 part1 YuChen Wu September 2020

1 problem1

(a) it is equal to

$$S_{2,-4} = \{2m - 4n : m, n \in Z\}$$

so we can take any m,n in Z as example,it might be -2(m=1,n=1),0(m=2,n=1), 2(m=3,n=1),4(m=4,n=1),6(m=5,n=1),...

(b) similarly

$$S_{12,18} = \{12m + 18n : m, n \in Z\}$$

the result can be -6(m=1,n=-1),6(m=-1,n=1),12(m=1,n=0),18(m=0,n=1),-12(m=-1,n=0),...

(c) i) assume

1)x,y=0 then d=0,z=0,d=z

2) when x or y$\neq$ 0 there must be a pair of n, m in Z that $mx + ny > 0$

$(if\ x\ or\ y < 0\ we\ can\ take\ m\ or\ n < 0\ and\ vice\ versa)$

hence there have positie number in $S_{x,y} \to z > 0$

$d = gcd(x, y) \to d|x$ and $d|y$

$\to d|(mx + ny)$ for $n, m \in Z$ (Divisibility)

$\to d|z$ (z is a number in $mx + ny$)

$\to dk = z$ ($k \in N^+$) ($z > 0$)

$\to z >= d$ ($k >= 1$)

combine two conditions $\to z >= d$ (d)

$i)\ \ 1)z = 0\ then\ x = 0, y = 0(\ similar\ to\ (c)(i)(2))$

$z|x\ and\ z|y$

$2)z \neq 0$

$assume\ that\ q = \lfloor \frac{x}{z} \rfloor = x\ div\ z$

$x\%z = x - (x\ div\ z)z = x - zq$

$= x - q(mx + ny)$

$= x(1 - qm) + y(-qn)\ which\ is\ also\ a\ combination\ of\ x\ and\ y$

$hence\ x\%z \in S_{x,y}$

because $0 \leq x\%z < z$ and z is already the positive smallest number

hence $x\%z = 0$

$\to x - pz = 0$ and p is a interger

$\to pz = x$ $\quad p \in N$

$\to z|x$

assume that $p = \lfloor \frac{y}{z} \rfloor = y$ div z

$y\%z = y - (y \text{ div } z)z = y - zq$

$= y - q(mx + ny)$

$= y(-qm) + y(1 - qn)$ which is also a combination of x and y

hence $y\%z \in S_{x,y}$

because $0 \leq y\%z < z$ and z is already the positive smallest number

hence $y\%z = 0$

$\to y - pz = 0$ and p is a interger

$\to pz = y$ $\quad p \in N$

$\to z|y$

ii)from i) we know z$|x$ and $z|y$
$hence\ z\ is\ a\ common\ divisor\ of\ x,y$
$while\ d\ is\ the\ greatest\ common\ divisor\ of\ x,y$
$hence\ d \geq z$

2 problem2

(a) if gcd(x,y)=1 it most exists wx+ny=1 w,n$\in Z$ $(B\acute{e}zout's\ identity)$
$and\ x,y\ can\ not\ be\ 0\ \sin ce\ gcd(0,t)=0$
$\rightarrow (-n)y = wx-1$
$n\ is\ a\ integer\ so\ -n\ is\ a\ integer$
$hence\ y|wx-1 \rightarrow wx\ = 1\ \ (mod\ y)\ \ \ (definition)$
$when\ wx+ny=1$
$set\ a\ t\ that\ (w+ty)x+(n-tx)y=1$
$w+ty\ could\ be\ a\ set\ that\ all\ subsets\ satified\ the\ condition$
$so\ there\ are\ at\ least\ one\ w_0 \in [0,\ y) \cap N\ when\ t = -\left\lfloor \frac{w}{y} \right\rfloor$
$(0\ \leq\ w\%y = w - \left\lfloor \frac{w}{y} \right\rfloor y\ <\ y\ )$
$(b)\ \ gcd(x,y)=1$
$\rightarrow it\ most\ have\ 1 = wx+ny\ \ \ \ w,n \in Z\ \ \ \ \ (B\acute{e}zout's\ identity)$
$\rightarrow k = k(wx+ny) = wkx+kny$
$y|kx\ and\ y|y$
$\rightarrow yt_1 = kx; y = y\ t_1 \in Z$
$\rightarrow (wt_1+kn)y = wkx+kny\ and\ wt_1+kn\ must\ be\ a\ integer$
$\rightarrow\ \ y|wkx+kny \rightarrow y|k$
(c) when wx=1 (mod y)
$\rightarrow wx-1 = 0\ (mod\ y)$
$\rightarrow y|wx-1$
$\rightarrow y|wx-(w_0x+n_0y)$
$\rightarrow y|(w-w_{0)}x+n_0y$
$\rightarrow y|(w-w_0)x$
$from\ (b)\ we\ know\ y|w-w_0\ which\ means$
$w = w_0\ (mod\ y) \rightarrow w = w_0+ky\ \ k \in Z$
$we\ have\ already\ know\ one\ w_a\ in\ (a)\ that\ satisfy\ the\ situation$
$w_0 = \frac{1-n_0y}{x}\ \ \ \ x,y\ are\ fixed\ number,\ when\ n_0\ changes$
$variance\ of\ w_0\ (\frac{t}{x}y) would\ always\ be\ a\ integer$
$when\ y\ is\ a\ integer,\ \frac{t}{x}\ is\ a\ integer$
$thus\ w = w_a+(k+\frac{t}{x})y$
$suppose\ k+\frac{t}{x} = p$
$it\ is\ clear\ that\ w = w_a+py\ (w \in [0,\ y) \cap N) could\ only\ have\ one\ solution$
$when\ w_a \in [0,y) \cap N\ \ \sin ce\ w_a+y \in [y,2y), w_a-y \in [-y,0)$

3 problem3

because m, n $\in \ N > 0, and\ m \geq n$
$0 \leq m\%n < n\ (lec2\ page44\ proofed\ in\ practice1)$
$n + m\%n < 2n$
$0 \leq \frac{3}{2}(n + m\%n) < (n + n) * \frac{3}{2} = 3n \leq m + 2n$
$then\ m + 0 = m + n\ (mod\ n)\ while\ n\ = 0\ (mod\ n)$
$thus\ (m + n)\%n = m\%n\ (lec02\ page43)$
$\frac{3}{2}(n + (m + n)\%n) = 3n \leq m + 2n$
$when\ n < m : \frac{3}{2}(n + (m + n)\%n) < m + 2n$
$we\ can\ assume\ m + n = t\ than$
$\frac{3}{2}(n + t\%n) < t + n$
$we\ can\ see\ m + n = t\ from\ anther\ point\ of\ view :$
$m\ as\ the\ gap\ between\ n\ and\ the\ target\ "m",\ t\ as\ our\ target\ "m"$
$then\ \frac{3}{2}(n + "m"\%n) < "m" + n$
$\sin ce\ m\ \in\ N > 0,\ \ now\ we\ only\ miss\ the\ case\ m = n$
$when\ m = n : \frac{3}{2}(n + m\%n) = \frac{3}{2}n < m + n = 2n$

4 problem4

(a)A$\oplus A$
$= (A \backslash A) \cup (A \backslash A) \quad (definition)$
$= (A \cap A^c) \cup (A \cap A^c) \quad (definition\ * 2)$
$= \emptyset \cup \emptyset \quad (complementation\ * 2)$
$= \emptyset$
$(b) A \cup u$
$= A \cup (A \cup A^c) \quad (complementation)$
$= A \cup (A^c \cup A) \quad (Commutativity)$
$= (A^c \cup A) \cup A \quad (Commutativity)$
$= A^c \cup (A \cup A) \quad (Associativity)$
$=\ A^c \cup A \quad (Idempotence : proof\ in\ lec03\ page79)$
$= A \cup A^c \quad (Commutativity)$
$= u \quad (Complementation)$

(c)A$\oplus B$
$= (A \backslash B) \cup (B \backslash A) \quad (definition)$
$= (A \cap B^c) \cup (B \cap A^c) \quad (definition)$
$= ((A \cap B^c) \cup B) \cap ((A \cap B^c) \cup A^c) \quad (Distributivity)$
$= (B \cup (A \cap B^c)) \cap (A^c \cup (A \cap B^c)) \quad (Commutativity * 2)$
$= ((B \cup A) \cap (B \cup B^c)) \cap ((A^c \cup A) \cap (A^c \cup B^c)) \quad (Distributivity * 2)$
$= ((B \cup A) \cap u) \cap (u \cap (A^c \cup B^c)) \quad (Complementation * 2)$
$= ((A \cup B) \cap u) \cap ((A^c \cup B^c) \cap u) \quad (Commutativity * 2)$
$= (A \cup B) \cap (A^c \cup B^c) \quad (Complementation * 2)$

(d)if x$\in (A \cup B)^C$:
$then\ x \notin (A \cup B) \qquad ((A \cup B) \cap (A \cup B)^c = \emptyset)$
$then\ x \notin A\ and\ x \notin B$
$if\ x \notin A\ then\ x \in A^c \qquad (A \cup A^c = u)$
$simliary\ x \in B^c$
$thus\ x \in B^c\ and\ x \in A^c$
$x \in (A^c \cap B^c)$
$thus\ (1)(A \cup B)^C \subseteq A^c \cap B^c$
$if\ x \in (A^c \cap B^c)$
$then\ x \in A^c\ and\ x \in B^c$
$it\ equals\ to\ x \notin A\ and\ x \notin B\ \sin ce\ (A \cap A^c = \emptyset, B \cap B^c = \emptyset)$
$thus\ x \notin (A \cup B)\ \rightarrow x \in (A \cup B)^c$
$(2)A^c \cap B^c \subseteq (A \cup B)^c$
$combine\ (1)and\ (2) \rightarrow\ A^c \cap B^c = (A \cup B)^c$

5 problem5

(a)false,for example when X={1},Y={0}
110 is a word in (X$\cup Y)^*\ \sin ce\ X \cup Y = \{0, 1\}$
$but\ not\ a\ word\ in\ X^*\ or\ Y^*$
$because\ we\ can\ not\ get\ 0, 1\ at\ the\ same\ time$
$(b)XY = \{xy : x \in X\ and\ y \in Y\}$
$XZ = \{xy : x \in X\ and\ y \in Z\}$
$(XY) \cup (XZ) = \{xy : x \in X\ and\ (y \in Z\ or\ y \in Y)\}(1)$
$Y \cup Z = \{y : y \in Z\ or\ y \in Y\}$
$thus\ X(Y \cup Z) = \{xy : x \in X\ and\ (y \in Z\ or\ y \in Y)\}\ which\ is\ equal\ to\ (1)$
$(c)X^* = X^0 \cup X^1 \cup X^2 \cup ...$
$X^0 = \{\lambda\}, X = X^1$
$X(X^*) = X^1 \cup X^2 \cup X^3 \cup ...$
$X^* \neq X(X^*)\ because,\ for\ example,\ when\ t = \lambda, X = \{a, b\}$
$X^* = \{\lambda, a, b, aa, bb, ab, aaa.....\}$
$X(X^*) = \{a, b, aa, bb, ab....\}$
$t \in X^*\ but\ t \notin X(X^*)$