Caleb Faruki
Dr. Xiaoxu Han
CISC4080 Algorithms
December 7, 2013

Homework 3

Part A

$If \quad a|b \quad a|c, \; then \; a|mb+nc, where\, m, n \in Z$

1.

$$If\; a|b, \; then \; b=ka \; for\, some \; k \in Z,$$
$$If\; a|c, \; then \; c=la \; for\, some \; l \in Z.$$
$$mb+nc = m(ka)+n(la) = \boldsymbol{a(mk+nl)}$$

$$(mk+nl) \in Z$$
$$substitute\, k, l \; with \; b, c$$
$$a|mk+nl \rightarrow \boldsymbol{a|mb+nc}$$

2.

$If \quad m|(a-b), \; then \; a \bmod m = b \bmod m, \; where \; m \in Z+¿\, a-b=km \rightarrow \boldsymbol{a=km+b}$

$$a \bmod m \;=\; (km+b) \bmod m \;=\; (km) \bmod m + (b) \bmod m$$
$$(km) \bmod m = 0, \; therefore \; \boldsymbol{a \bmod m = b \bmod m}$$

3.

$$If \quad a \bmod m = b \bmod m \quad for \quad m \in Z+, \; then:$$
$$a = km+r \quad k \in Z, \; 0 \le r < m,$$
$$b = lm+r \quad l \in Z, \; 0 \le r < m,$$

$$a-b \;=\; (km+r)-(lm+r)$$
$$= \; km+r - lm - r$$
$$= \; km - lm$$
$$= \; m(k-l), \; where \; (k-l) \in Z$$

$Therefore, \; if\, a \bmod m \,=\, b \bmod m \quad for \quad m \in Z+, \; then \; \boldsymbol{m \in (a-b)}$