Written Homework 2 Solution

1.

a) (10 pts, 5 pts for each book)

Book 1: **Essentials of programming languages**
ISBN: **0262062178**
(1*0+2*2+3*6+4*2+5*0+6*6+7*2+8*1+9*7+10*8) mod 11
= (0+4+18+8+0+36+14+8+63+80) mod 11
= 231 mod 11
=0

Book 2: **The Scheme programming language**
ISBN: **013791864X**
(1*0+2*1+3*3+4*7+5*9+6*1+7*8+8*6+9*4+10*10) mod 11
= (0+2+9+28+45+6+56+48+36+100) mod 11
= 330 mod 11
=0

b) (5 pts)
0-471-52713-C
(1*0+2*4+3*7+4*1+5*5+6*2+7*7+8*1+9*3+10*C) mod 11
= (0+8+21+4+25+12+49+8+27+10C) mod 11
= (154+10C) mod 11
=0
154 mod 11=0, so 10C mod 11=0
C=0

c) (5 pts)
0-553-5D331-4
(1*0+2*5+3*5+4*3+5*5+6*D+7*3+8*3+9*1+10*4) mod 11
= (0+10+15+12+25+6D+21+24+9+40) mod 11
= (156+6D) mod 11
=0
156 mod 11 =2, so 6D mod 11 =9
D= 7

2. (5 pts)
Proof:
What we trying to prove could be restated as below because of “if only if”:

$$f(x) = x \quad \text{for some x in } Zn \text{ iff } \quad \gcd(a-1, n) \mid b$$

So, we have:

$$f(x) = (ax + b) \bmod n = x$$
$$(ax + b) \bmod n = x \bmod n$$
$$(ax - x + b) \bmod n = (x - x) \bmod n$$
$$((a-1)x + b) \bmod n = 0 \bmod n$$
$$((a-1)x + b - b) \bmod n = (0 - b) \bmod n$$
$$(a-1)x \bmod n = (-b) \bmod n$$
$$(a-1)x \bmod n = n - b$$

Since we also have the fact that,

The equation $ax \bmod n = b$ **has a solution x iff** $\gcd(a, n) \mid b$

So, we have

$(a-1)x \bmod n = n - b$ has a solution x iff $\gcd(a-1, n) \mid n - b$

we also know that

$\gcd(a-1, n)$ is the a divisor of n, so $\gcd(a-1, n) \mid n$

So we have

$$\gcd(a-1, n) \mid n - (n - b)$$
$$\gcd(a-1, n) \mid b$$

3.

a) (5 pts)

Proof:

$\gcd(a, 26) = 1 \mid b$ iff $ax \bmod 26 = b$ has a solution x

Since 1 divides every number, for any $0 \le b \le 25$, $ax \bmod 26 = b$ has a solution x

That means the value of $ax \bmod 26$ is distinct

The value of $c(x) = (ax + b) \bmod 26$ is distinct for any fixed b.

b) (10 pts)

According to the facts we have proved above, we have

$\gcd(a, 26) = 1$ and $\gcd(a-1, 26)$ doesn't divide b to insure that all the values of

$C(x)$ for $0 \le x \le 25$ are distinct and $C(x) \ne x$ for any x.

For all odd numbers of $1 \le b \le 25$, we get all odd numbers $1 \le a \le 25$ except 13.

For all even numbers of $0 \le b \le 24$, no a will fits the requirement.