姓名:胡劭 系級:資工碩一 學號:M11215075

1. Answer each the following questions:

   (a) Prove that if $a > b > 0$ and $c = a + b$, then $c \bmod a = b$.

   (b) Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Sol:

a. c mod a = a + b mod a

= (a mod a) + (b mod a)

= 0 + b = b

可以用除法定理來看

c = 1 x a + b 所以當 c 除以 a 時候 餘數為 b #QED

b.

令 a,b,c 為整數，其中$a \neq 0$，根據定義 a|b 意思是 b 是 a 的倍數。

$\therefore b = a \times x$ 且$c = b \times y$

$\because b = a \times x \therefore c = a(xy)$

故 c 是 a 的倍數-> a | c #QED

2. Compute the values $(d, x, y)$ that the call EXTENDED-EUCLID(899, 493) returns.

$$\begin{pmatrix} 899 & 493 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 406 & 493 \\ 1 & 0 \\ -1 & 1 \end{pmatrix} \to \begin{pmatrix} 406 & 87 \\ 1 & -1 \\ -1 & 2 \end{pmatrix}$$

$$\to \begin{pmatrix} 58 & 87 \\ 5 & -1 \\ -9 & 2 \end{pmatrix} \to \begin{pmatrix} 58 & 29 \\ 5 & -6 \\ -9 & 11 \end{pmatrix} \to \begin{pmatrix} 0 & 29 \\ 17 & -6 \\ -31 & 11 \end{pmatrix}$$

$$17 \times 899 + 493 \times -31 = 0$$
$$-6 \times 899 + 11 \times 493 = 29$$

$$(29, -6, 11) \#$$

3. Prove that if $a$ and $b$ are any positive integers such that $a \mid b$, then

$$(x \bmod b) \bmod a = x \bmod a$$

for any $x$. Prove, under the same assumptions, that

$$x = y \pmod b \text{ implies } x = y \pmod a$$

for any integers $x$ and $y$.

3.1 if $a$ & $b \in \mathbb{Z}^+$, s.t $a|b \to (x \text{ mob } b) \bmod a = x \bmod a$, for any $x$

$a | b \Rightarrow b = ak$

令 $x = qb + r$, for any $x$, 其中 $0 \le r < b$

$\because (x \bmod b) \bmod a = r \bmod a$

$\therefore x \bmod a \Rightarrow (qb + r) \bmod a = qb \bmod a + r \bmod a$

$\because a \mid b \Rightarrow qb \bmod a = 0$

$\therefore x \bmod a = r \bmod a$

故 $(x \bmod b) \bmod a = r \bmod a$,

$= x \bmod a$ #QED

3.2 3.1 已証出是對的,則

if $x \equiv y \pmod b \to x \equiv y \pmod a$ for all $x, y \in \mathbb{Z}$

$x \equiv y \pmod b \Rightarrow b \mid x - y \Rightarrow x - y = qb$

$\because b = ak$

$\therefore x - y = qak = (qk)a$

$\therefore a | x - y \Rightarrow x \equiv y \bmod a$ #QED

4. Prove that if $p$ is prime and $0 < k < p$, then $p \mid \begin{pmatrix} p \\ k \end{pmatrix}$. Calculate that for all integers $a, b$ and primes $p$,

$$(a+b)^p = a^p + b^p \pmod{p}$$

$$\binom{P}{k} = \frac{P!}{k!(P-k)!} = \frac{P(P-1)!}{k!(P-k!)} = P \times \frac{(P-1)!}{k!(P-k!)} = Pt$$

$\because \binom{P}{k}$ 是 P 的整數倍

$\therefore P \mid \binom{P}{k}$ #QED

by 2 項式定理

$$(a+b)^P = \sum_{k=0}^{P} \binom{P}{k} a^k b^{P-k}$$

$$\Rightarrow \binom{P}{0} a^0 b^P + \binom{P}{1} a^1 b^{P-1} + \cdots + \binom{P}{P} a^P b^0 \pmod{P}$$

$$\equiv b^P + \binom{P}{1} a^1 b^{P-1} + \cdots + a^P \pmod{P}$$

$$\equiv b^P + 0 + \cdots + 0 + a^P \pmod{P}$$

$$\equiv a^P + b^P \pmod{P} \quad *$$

5. Answer the following questions:

(a) Find all solutions to the equation $35x = 10 \pmod{50}$.

(b) Find all solutions to the equations $x = 4 \pmod{5}$ and $x = 5 \pmod{11}$.

Sol:

(a) 50 | 35x -10 => 50k = 35x -10 => 35x − 50k = 10

50 = 35*1 + 15

35 = 15*2 + 5

15 = 5*3 + 0

⇨ 5 = 35 − 15*2 = 35 − (50 − 35*1)*2 = 35 − 2*50 + 2*35 = -2*50 + 3*35

同乘 2

⇨ 10 = -4*50 + 6*35

⇨ 6*35 ≡ 10 (mod 50)

∴x ≡ 6 (mod50)

i.e. x = 6 + 50k, ∀k ∈ ***Z***

(b)令 r1 = 4, r2 = 5

n1 = 5, n2 = 11

n = 5 * 11 = 55

N1 = $\frac{\mathrm{n}}{n1} = \frac{55}{5} = 11$ N2 = $\frac{\mathrm{n}}{n2} = \frac{55}{11} = 5$

$\mathrm{M1} \equiv N1^{-1}\ (mod\ n1) \equiv 1$

$\mathrm{M2} \equiv N2^{-1}\ (mod\ n2) \equiv 9$

x ≡ r1M1N1 + r2M2N2 (mod 55)

≡ 44 + 225 (mod 55)

≡ 269 (mod 55)

≡ 49 (mod 55)

∴ x = 49 + 55k, ∀k ∈ ***Z***