MF IN FINTECH

谢泽健
11810105

HW2

2019.7.7

Part 1

Q.1 Suppose that A, B and C are three finite sets. For each of the following, determine whether or not it is true. Explain your answers.

a.

True

$$A = (A \cap B) \cup (A - B) \tag{1}$$

$$\emptyset = (A \cap B) \cap (A - B) \tag{2}$$

If $A - B = A$:

$$A = (A \cap B) \cup A \tag{3}$$

$(A \cap B)$ must be $\emptyset$, otherwise $(A \cap B) \cap A$ can't be $\emptyset$, but we know that

$$A \cap B \neq \emptyset \tag{4}$$

$$\therefore \quad A - B \neq A \tag{5}$$

Then, since

$$A - B \in A \tag{6}$$

We conclude that

$$A - B \notin A \tag{7}$$

b.

False

Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. $A - B = A$ but $B \notin A$.

c.

True

$A \cap B = B \cap A$ is always true, which leads to that statement is also true.

d.

False

Let $A = B = \{1, 2, 3\}$, $|A \cup B| = |A| = 3 < 2|A| = 6$

e.

True

$$A \cap B \cap C \subseteq A \subseteq (A \cup B) \tag{8}$$

f.

False

$$\overline{(A - B)} \cap (B - A) \subseteq (B - A) \subseteq B \tag{9}$$

Q.2 For each set defined below, determine whether the set is countable or uncountable. Explain your answers. Recall that N is the set of natural numbers and R denotes the set of real numbers

a.

countable, which is a finite set

b.

countable, since N is a countable set, we can list its elements: a_1, a_2, a_3 ..., hence we can list (a, b) as follows:

$$(a_1, a_1), (a_1, a_2), (a_2, a_1), (a_1, a_3), (a_2, a_2), (a_3, a_1) \ldots (a_i, a_j) \tag{10}$$

where $i + j = 2, 3, 4 \ldots$

c.

uncountable.

$$|N \times R| \leq |R| \tag{11}$$

since R is uncountable, so $N \times R$ is.

Q.3 Give an example of two uncountable sets A and B such that the intersection $A \cap B$ is

a.

$$\begin{cases} A = [-1, 0] \\ B = [0, 1] \end{cases} \tag{12}$$

b.

$$\begin{cases} A = [-1, 0] \bigcup N \\ B = [0, 1] \bigcup N \end{cases} \tag{13}$$

c.

$$\begin{cases} A = [-1, 1] \\ B = [0, 1] \end{cases} \tag{14}$$

Q.4 Prove the following using set identities

a.

$$(B - A) \bigcup (C - A) = \left(B \bigcap A^c\right) \bigcup \left(C \bigcap A^c\right) = A^c \bigcap \left(B \bigcup C\right) = \left(B \bigcup C\right) - A \tag{15}$$

b.

$$A \bigcap B \bigcap \overline{B \bigcap C} \bigcap A \bigcap C = A \bigcap \left(B \bigcap C\right) \bigcap \overline{B \bigcap C} = A \bigcap \emptyset = \emptyset \tag{16}$$

Q.5 For each of the following mappings, indicate what type of function they are (if any). Use the following options to describe them, and explain your answers.
i. Not a function.
ii. A function which is neither one-to-one nor onto.
iii. A function which is onto but not one-to-one.
iv. A function which is one-to-one but not onto.
v. A function which is both one-to-one and onto.

a.

iv.

The function is one-to-one, because if $f(x_1) = f(x_2)$:

$$2|x_1| = 2|x_2| \Rightarrow x_1 = x_2 \tag{17}$$

The function is not onto, for the odd number in $\mathbb{Z}$, no exist $x \in \mathbb{Z}$, $f(x)$ equals it.

b.

i.

For $x = 3$, $f(x)$ is not in $\{2, 4\}$

c.

v.

The function is one-to-one, because if $f(x_1) = f(x_2)$:

$$8 - 2x_1 = 8 - 2x_2 \Rightarrow x_1 = x_2 \tag{18}$$

The function is onto because $\forall y \in \mathbb{R},\ \exists x = \frac{8-y}{2}$, let $f(x) = y$.

d.

iii.

The function is not one to one, because $f(0.1) = f(0.2)$

The function is onto because $\forall y \in Z,\ f(y - 1) = y$

e.

i.

For $x < 1$, $f(x)$ is not in $\mathbb{R}^+$.

f.

iv.

The function is one-to-one, because if $f(x_1) = f(x_2)$:

$$x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2 \tag{19}$$

The function is not onto, because for $y = 1$, there is not such $x \in \mathbb{Z}^+$ let $f(x) = y$.

Q.6 Prove that P(A) ⊆ P(B) if and only if A ⊆ B

If $A \subseteq B$, for every set x in $P(A)$, they are subset of A:

$$\forall x \in P(A)\ x \subseteq A \subseteq B \Rightarrow \forall x \in P(A),\ x \in P(B) \Rightarrow P(A) \subseteq P(B) \tag{20}$$

If $P(A) \subseteq P(B)$, note:

$$A \in P(A) \Rightarrow A \in P(B) \Rightarrow A \subseteq B \tag{21}$$

Q.7 Show that if A, B and C are sets, then

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{22}$$

Therefore

$$|(A \cup B) \cup C)| = |A \cup B| + |C| - |(A \cup B) \cap C| = |A| + |B| - |A \cap B| + |C| - |(A \cup B) \cap C| \tag{23}$$

$$|(A \cup B) \cap C| = |(A \cap C) \cup (B \cap C)| = |A \cap C)| + |B \cap C)| - |A \cap B \cap C| \tag{24}$$

Then

$$|(A \cup B) \cup C)| = |A| + |B| - |A \cap B| - |A \cap C)| - |B \cap C)| + |A \cap B \cap C| \tag{25}$$

Q.8 Suppose that f is an invertible function from Y to Z and g is an invertible function from X to Y . Show that the inverse of the composition f ∘g is given by

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

For any $(f \circ g)(x) = y$, i.e.

$$f(g(x)) = y \tag{26}$$

$$g(x) = f^{-1}(y) \tag{27}$$

$$x = g^{-1}(f^{-1}(y)) = (g^{-1} \circ f^{-1})(y) \tag{28}$$

since

$$x = (f \circ g)^{-1}(y) \tag{29}$$

we concluded that

$$(f \circ g)^{-1} = \left(g^{-1} \circ f^{-1}\right) \tag{30}$$

Q.9 Let x be a real number. Show that

i.

$$x = \lfloor x \rfloor + \{x\} \tag{31}$$

If $\{x\} \in [0,\ 1/3)$

$$\lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor = \lfloor x \rfloor + \lfloor x \rfloor + \lfloor x \rfloor = 3 \lfloor x \rfloor \tag{32}$$

$$\lfloor 3\,x \rfloor = \lfloor 3 \lfloor x \rfloor + 3 \{x\} \rfloor = 3 \lfloor x \rfloor \tag{33}$$

ii.

If $\{x\} \in [1/3,\ 2/3)$

$$\lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor = \lfloor x \rfloor + \lfloor x \rfloor + \lfloor x \rfloor + 1 = 3 \lfloor x \rfloor + 1 \tag{34}$$

$$\lfloor 3\,x \rfloor = \lfloor 3 \lfloor x \rfloor + 3 \{x\} \rfloor \tag{35}$$

Note

$$1 \le 3 \{x\} < 2 \Rightarrow \lfloor 3 \lfloor x \rfloor + 1 \rfloor \le \lfloor 3 \lfloor x \rfloor + 3 \{x\} \rfloor < \lfloor 3 \lfloor x \rfloor + 2 \rfloor \tag{36}$$

hence

$$\lfloor 3\,x \rfloor = 3 \lfloor x \rfloor + 1 \tag{37}$$

iii.

If $\{x\} \in [2/3,\ 1)$

$$\lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor = \lfloor x \rfloor + \lfloor x \rfloor + 1 + \lfloor x \rfloor + 1 = 3 \lfloor x \rfloor + 2 \tag{38}$$

$$\lfloor 3\,x \rfloor = \lfloor 3 \lfloor x \rfloor + 3 \{x\} \rfloor \tag{39}$$

Note

$$2 \le 3 \{x\} < 3 \Rightarrow \lfloor 3 \lfloor x \rfloor + 2 \rfloor \le \lfloor 3 \lfloor x \rfloor + 3 \{x\} \rfloor < \lfloor 3 \lfloor x \rfloor + 3 \rfloor \tag{40}$$

hence

$$\lfloor 3\,x \rfloor = 3 \lfloor x \rfloor + 2 \tag{41}$$

Then we concluded that

$$\lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor = \lfloor 3\,x \rfloor \tag{42}$$

Q.10 Derive the formula for

Note

$$(n+1)^3 - n^3 = 1 + 3\,n + 3\,n^2 \tag{43}$$

hence

$$(n+1)^3 = \sum_{i=0}^{n} 1 + 3\,i + 3\,i^2 \tag{44}$$

Simply:

$$\sum_{i=0}^{n} i^2 = \left((n+1)^3 - \sum_{i=0}^{n} 1 + 3\,i\right) \Big/ 3 = \left((n+1)^3 - \frac{1}{2}(1+n)(2+3\,n)\right) \Big/ 3 = \frac{1}{6} n \left(1 + 3\,n + 2\,n^2\right) \tag{45}$$

Q.11 Show that a subset of a countable set is also countable

If a set A is countable, there exist a function from A to $\mathbb{Z}$, for any subset in A, the function also map this subset to $\mathbb{Z}$, hence the subset is also countable.

Q.12 If A is an uncountable set and B is a countable set, must A − B be uncountable?

We know that countable countable sets is still countable. If $A - B$ is countable, $(A - B) \bigcup B$ is also countable, however $(A - B) \bigcup B$ is actually A and which is uncountable.

Q.13 Suppose that f(x), g(x) and h(x) are functions such that f(x) is Θ(g(x)) and g(x) is Θ(h(x)). Show that f(x) is Θ(h(x)).

There exist $m,\ n,\ p,\ q$, let

$$\forall\, x > x_1\ m\,|g(x)| \le |f(x)| \le n\,|g(x)| \tag{46}$$

$$\forall\, x > x_x\ p\,|h(x)| \le |g(x)| \le q\,|h(x)| \tag{47}$$

Hence, let $x_0 = \max(x_1,\ x_2)$, $\forall\, x > x_0$

$$mp\,|h(x)| \le |f(x)| \le nq\,|h(x)| \tag{48}$$

Then we concluded that

$$f(x) = \Theta(h(x)) \tag{49}$$

Q.14 If f1(x) and f1(x) are functions from the set of positive integers to the set of positive real numbers and f1(x) and f2(x) are both Θ(g(x)), is (f1 − f2)(x) also Θ(g(x))? Either prove that it is or give a counter example.

No.

For instance, let

$$f_1(x) = f_2(x) = 3\,x \tag{50}$$

$f_1(x)$ and $f_2(x)$ are both $\Theta(x)$, however

$$(f_1 - f_2)\,(x) = 0 \tag{51}$$

which is not $\Theta(x)$.

Q.15 Show that if

$$f(x) = a_{n-1}\,x^{n-1} + a_n\,x^n + a_1\,x + a_0 + \cdots$$

where a0, a1, . . . , an−1,and an are real numbers and an 6= 0, then f(x) is Θ(x^n).

There exist x_0, let $\forall\, x > x_0$

$$|f(x)| \le |a_n|\,x^n + |a_{n-1}|\,x^n + \ldots + |a_1|\,x^n + |a_0|\,x^n = \sum_{i=0}^{n} |a_i|\,x^n \tag{52}$$

so $f(x)$ is $O(x^n)$.

Note:

$$|f(x)| = x^n \left| \sum_{i=0}^{n} \frac{a_{n-i}}{x^i} \right| \tag{53}$$

Let $m = \max(a_0,\ a_2,\ \ldots,\ a_{n-1})$, $\forall\, x > \max\left(1,\ \frac{2\,mn}{|a_n|}\right)$

$$0 < |a_{n-i}/x^i| \leq \frac{|a_n|}{2\,n} \tag{54}$$

hence

$$\left|\sum_{i=0}^{n} a_{n-i}/x^i\right| \geq \frac{|a_n|}{2} \tag{55}$$

so $f(x)$ is $\Omega(x^n)$.

Q.16 Show that n log n is O(log n!).

Note:

$$\sum_{i=1}^{n} \ln(x) > \int_1^n \ln(x)\,dx = 1 - n + n\ln(n) \tag{56}$$

When $n > e^2$:

$$n\ln(n) > 2\,(n-1) \tag{57}$$

Hence, $\forall\ n > e^2$

$$2\,\ln(n!) > 2\,(1-n) + 2\,n\ln(n) > n\ln(n) \tag{58}$$

i.e.

$$\forall\ n > e^2\ |n\ln(n)| < 2\,|\ln(n!)| \Rightarrow n\ln(n) = O(\ln(n!)) \tag{59}$$

Q.17

(a) Show that this algorithm determines the number of 1 bits in the bit string S:

Consider the rightmost and longest substring of the bit string which contains only one 1:

"000...1...000" (60)

When $S - 1$, This substring will become

"000...0...111" (61)

The 0 at the left side will still 0 while the 0 at the right side will become 1, 1 will become 0. Then

"000...1...000"

∧

“000...0...111”

"000...0...000" (62)

The substring is all 0.

That is, the operation in the loop body let add 1 up to count and make the substring which contains 1 becomes a substring of next substring.

(b) How many bitwise AND operations are needed to find the number of 1 bits in a string S using the algorithm in part a)?

Suppose the length of S is n and the number of 1's is m, for each loop, need n bitwise AND operation, so it need nm in total.

Q.18 The conventional algorithm for evaluating a polynomial anxn+an−1xn−1+· · · a1x+a0 at x = c can be expressed in pseudocode by where the final value

At each loop, there is 2 multiplications and 1 additions, so from $i = 1$ to $i = n$, there is 2 n multiplications and n additions in total.

Q.19 There is a more efficient algorithm (in terms of the number of multiplications and additions used) for evaluating polynomials than the conventional algorithm described in the previous exercise. It is called Horner’s method. This pseudocode shows how to use this method to find the value of anxn + an−1xn−1 + · ·· + a1x + a0 at x = c.

This algorithm is actually evaluate this sequence:

$$b_n = a_n$$
$$b_{n-1} = a_{n-1} + b_n\, c$$
$$\vdots$$
$$b_0 = a_0 + b_1\, c$$

From b_0 to b_{n-1}, there is n multiplications and n additions.

Part 2

Q.1 What are the prime factorizations of

a.

$$511 = 7\times 73 \tag{63}$$

b.

$$12 = 2^{10}\times 3^5\times 5^2\times 7\times 11 \tag{64}$$

Q.2

a.

$$\text{GCD}(561,\ 234) = \text{GCD}(93,\ 234) = \text{GCD}(93,\ 48) = \text{GCD}(45,\ 48) = 3 \tag{65}$$

b.

$$3 = -5\times 561 + 12\times 234 \tag{66}$$

Q.3 Prove the following statements.

a.

$$c\,|\,ab \Rightarrow c\,|\,a\,\text{GCD}(b,\ c)\,\frac{b}{\text{GCD}(b,\ c)} \tag{67}$$

Note

$$\text{GCD}\left(c,\ \frac{b}{\text{GCD}(b,\ c)}\right) = 1 \tag{68}$$

then we concluded that $c\,|\,a\,\text{GCD}(b,\ c)$

b.

There exist integer $m,\ n,\ k$, let

$$a = md_1,\ b = nd_2,\ y = ((d_1\ d_2)/\text{GCD}(d_1,\ d_2))\ k \tag{69}$$

where $\text{GCD}(m,\ k) = 1$ and $\text{GCD}(n,\ k) = 1$

Then

$$\text{GCD}(\text{GCD}(a,\ b),\ y) = \text{GCD}(\text{GCD}(md_1,\ nd_2),\ ((d_1\ d_2)/\text{GCD}(d_1,\ d_2))\ k) \tag{70}$$

Obviously, $\text{GCD}(d_1,\ d_2)$ is a common divisor of $\text{GCD}(md_1,\ nd_2)$ and $\frac{d_1\ d_2}{\text{GCD}(d_1,d_2)}\ k$, the we prove it's greatest.

If there exist prime p such that:

$$p\,\text{GCD}(d_1,\ d_2)\,|\,\text{GCD}(md_1,\ nd_2)\ \text{and}\ p\,\text{GCD}(d_1,\ d_2)\,|\,(d_1\ d_2)/\text{GCD}(d_1,\ d_2)\ k \tag{71}$$

Note:

$$p\,|\,ab \Rightarrow p\,|\,a\ \vee\ p\,|\,b\ \text{is alwalys true.} \tag{72}$$

hence

$$p\,|\,m,\ p\,|\,m,\ p\,|\,k \tag{73}$$

that is p is a common divisor, however GCD(m, k) = 1 and GCD(n, k) = 1, so there is no such p. Then we concluded that

$$\text{GCD}(\text{GCD}(md_1,\, nd_2),\, ((d_1 = d_2)/\text{GCD}(d_1,\, d_2))\, k) = \text{GCD}(d_1,\, d_2) \tag{74}$$

c.

$$\text{GCD}(a + b,\, b - a) = \text{GCD}(b + a,\, 2\, a) \tag{75}$$

First, let $b = 3,\ a = 1$:

$$\text{GCD}(b + a,\, 2\, a) = \text{GCD}(4,\, 2) = 2 \tag{76}$$

Then we prove that GCD ($b + a$, 2 a) can't greater than 2.

If there exist a prime $p > 2$, such that

$$p \mid 2\, a,\ p \mid b + a \tag{77}$$

since $p > 2$, p is not divisible 2, so $p \mid a$ and $p \mid b$, that is

$$\text{GCD}(a,\, b) \geq p \tag{78}$$

however GCD(a, b) is actually 1, so there is no such p. Hence

$$\text{GCD}(a + b,\, b - a) = \text{GCD}(b + a,\, 2\, a) \leq 2 \tag{79}$$

Q.4 Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if an−1 ≡ 1 (mod n).

a.

Pass

$$2^{560} \equiv 1 \pmod{561} \tag{80}$$

b.

No

$$561 = 3 \times 11 \times 17 \tag{81}$$

Q.5 Solve the following modular equations.

a.

$$\text{GCD}(267,\, 79) = 1 \tag{82}$$

The modular equation has a unique solution

The inverse of 267 mod 79 is:

$$269 \times 29 \equiv 1 \pmod{79} \tag{83}$$

So the solution is:

$$x = 87 + 79\, t (t \in \mathbb{Z}) \tag{84}$$

b.

$$\text{GCD}(778,\, 379) = 1 \tag{85}$$

The modular equation has a unique solution

The inverse of 267 mod 79 is:

$$778 \times 19 \equiv 1 \pmod{379} \tag{86}$$

So the solution is:

$$x = 190 + 379\, t (t \in \mathbb{Z}) \tag{87}$$

c.

$$\text{GCD}(312,\, 97) = 1 \tag{88}$$

The modular equation has a unique solution

The inverse of 312 mod 97 is:

$$312 \times 37 \equiv 1 \pmod{97} \tag{89}$$

So the solution is:

$$x = 111 + 97\,t (t \in \mathbb{Z}) \tag{90}$$

Q.6 Let a and b be positive integers. Show that gcd(a, b) + lcm(a, b) = a + b if and only if a divides b, or b divides a.

$$\mathrm{GCD}(a,\, b) + \mathrm{LCM}(a,\, b) = a + b \tag{91}$$

$$\mathrm{GCD}(a,\, b)\,\mathrm{LCM}(a,\, b) = ab \tag{92}$$

Suppose equation

$$x^2 - (a + b)\,x + ab = 0 \tag{93}$$

Which has only 2 solutions, that is

$$\mathrm{GCD}(a,\, b) = a \text{ or } \mathrm{GCD}(a,\, b) = b \tag{94}$$

i.e. a divides b, or b divides a.

Q.7 Prove that if a and m are positive integer such that gcd(a, m) = 1 then the function f : {0, . . . , m − 1} → {0, . . . , m − 1} defined by f(x) = (a · x) mod m is a bijection.

The domain and the codomain are the same, so we only to prove that this function is one-to-one, suppose:

$$ax_1 \bmod m = ax_2 \bmod m \tag{95}$$

it derives:

$$m \,|\, a(x_1 - x_2) \tag{96}$$

since

$$\mathrm{GCD}(a,\, m) = 1 \tag{97}$$

hence

$$x_1 \equiv x_2 (\mathrm{mod}\, m) \Rightarrow x_1 = x_2 \tag{98}$$

Q.8Prove that if a and m are positive integers such that gcd(a, m) ≠ 1 then a does not have an inverse modulo m.

There is integer s and t such that

$$sa + tm = \mathrm{GCD}(a,\, m) \tag{99}$$

which implies

$$sa + tm \equiv \mathrm{GCD}(a,\, m) \pmod{m} \tag{100}$$

Note

$$tm \equiv 0 \pmod{m} \tag{101}$$

∴

$$sa \equiv \mathrm{GCD}(a,\, m) \pmod{m} \tag{102}$$

However, we know that GCD $(a,\, m)$ is the minimum for all s and t

$$sa \equiv \mathrm{GCD}(a,\, m) > 1 \pmod{m} \tag{103}$$

so a does not have an inverse modulo m.

Q.9Prove that if m is a positive integer of the form 4k + 3 for some nonnegative integer k, then m is not the sum of the squares of two integers.

It's equivalent to prove that, there is no $a,\ b$ such that

$$a^2 + b^2 \equiv 3 \pmod 4 \tag{104}$$

Suppose any integer x, the set of x mod 4 is

$$\{x \mid x = a \bmod 4\} = \{0,\ 1,\ 2,\ 3\} \tag{105}$$

it derives:

$$\left\{x \mid x = a^2 \bmod 4\right\} = \{0,\ 1\} \tag{106}$$

for any two elements of this set, their sum can't equal to 3.

Q.10 Find counterexamples to each of these statements about congruences.

a.

Let $a = 3,\ b = 5,\ c = 2,\ m = 4$:

$$3 \times 2 \equiv 5 \times 2 \equiv 2 \pmod 4 \tag{107}$$

but

$$3 \not\equiv 5 \pmod 4 \tag{108}$$

b.

Note

$$2 \equiv 5 \pmod 3 \tag{109}$$

Let $a = d = 2,\ b = c = 5$:

$$2^5 \equiv 2 \pmod 3 \tag{110}$$

$$5^2 \equiv 1 \pmod 3 \tag{111}$$

Q.11 Convert the decimal expansion of each of these integers to a binary expansion.

a.

$$321 = (101\,000\,001)_2 \tag{112}$$

b.

$$1023 = (1\,111\,111\,111)_2 \tag{113}$$

c.

$$100\,632 = (11\,000\,100\,100\,011\,000)_2 \tag{114}$$

Q.12 Show that log2 3 is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.

If there is m and n such that

$$\log_2 3 = \frac{n}{m} \tag{115}$$

It's equivalent

$$2^n = 3^m \tag{116}$$

Note 2^n is always even number for $n > 0$, and 3^m is always odd number. So $n = m = 0$, however $\frac{n}{m}$ is not exist when $m = 0$.

Q.13 Prove that there are infinitely many primes of the form 4k + 3, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes q1, q2, . . . , qn, and consider the number 4q1q2 · · · qn − 1

Note the set

$$\{4k+1 \mid k \in \mathbb{Z}^+\} \tag{117}$$

is closed by multiplication.

Consider the number

$$4n! - 1 \equiv 3 \pmod 4 \tag{118}$$

whose prime factors can't all of this form $4k + 1$. So there is a prime $p = 4k - 1$, such that

$$p \mid 4n! - 1 \tag{119}$$

Since for any prime p' smaller than n

$$p' \nmid 4n! - 1 \tag{120}$$

So we can say for any n, there exist a prime greater than n and of the form $4k + 3$.

Q.14 Solve the system of congruence x ≡ 3 (mod 6) and x ≡ 4 (mod 7) using the methods of Chinese Remainder Theorem or back substitution.

$$M = 6 \times 7 = 42 \tag{121}$$

$$M_1 = \frac{M}{m_1} = \frac{42}{6} = 7 \tag{122}$$

$$M_2 = m_1 = 6 \tag{123}$$

Find the modulo inverse:

$$\begin{cases} 7s_1 \equiv 1 \pmod 6 \\ 6s_2 \equiv 1 \pmod 7 \end{cases} \Rightarrow \begin{cases} s_1 = 1 \\ s_2 = 6 \end{cases} \tag{124}$$

So the solution is

$$x_0 = 7 \times 1 \times 3 + 6 \times 6 \times 4 = 165 + 42t \, (t \in \mathbb{Z}) \tag{125}$$

Q.15 Find all solutions, if any, to the system of congruences x ≡ 5 (mod 6), x≡ 3 (mod 10), and x ≡ 8 (mod 15).

$$\text{GCD}(6,\ 10,\ 15) = 30 \tag{126}$$

Test from 1 to 30, the only solution is 23.

$$x = 23 + 30t \, (t \in \mathbb{Z}) \tag{127}$$

Q.16 Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of (p − 1)(q − 1).

Expand $(p - 1)(q - 1)$:

$$(p-1)(q-1) = pq - (p+q) + 1 \tag{128}$$

So we can get $s = p + q$ easily. Then we know that

$$n = pq = p(s - p) \tag{129}$$

i.e.

$$p^2 - ps + n = 0 \tag{130}$$

So

$$p = \frac{s \pm \sqrt{s^2 - 4n}}{2} \tag{131}$$

Then we can get q.