Discrete Mathematics(H)
Southern University of Science and Technology
Mengxuan Wu
12212006

Assignment 3

Mengxuan Wu

Q.1

(a)

$$
\begin{aligned}
12! =& 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \\
=& (2^2 \times 3) \times 11 \times (2 \times 5) \times 3^2 \times 2^3 \times 7 \times (2 \times 3) \times 5 \times 2^2 \times 3 \times 2 \times 1 \\
=& 2^{10} \times 3^5 \times 5^2 \times 7 \times 11
\end{aligned}
$$

(b)

$$
\begin{aligned}
6560 =& 2 \times 3280 \\
=& 2^2 \times 1640 \\
=& 2^3 \times 820 \\
=& 2^4 \times 410 \\
=& 2^5 \times 205 \\
=& 2^5 \times 5 \times 41
\end{aligned}
$$

Q.2

(a)

$$
\begin{aligned}
312 =& 2 \times 156 \\
=& 2^2 \times 78 \\
=& 2^3 \times 39 \\
=& 2^3 \times 3 \times 13
\end{aligned}
$$

(b)

$$
\begin{aligned}
312 \div 97 =& 3...21 \\
97 \div 21 =& 4...13 \\
21 \div 13 =& 1...8 \\
13 \div 8 =& 1...5 \\
8 \div 5 =& 1...3 \\
5 \div 3 =& 1...2 \\
3 \div 2 =& 1...1 \\
2 \div 1 =& 2...0
\end{aligned}
$$

Therefore, $\gcd(312, 97) = 1$.

(c)

$$
\begin{aligned}
1 =& 3 - 1 \times 2 \\
=& 3 - 1 \times (5 - 3) & =& 2 \times 3 - 1 \times 5 \\
=& 2 \times (8 - 5) - 1 \times 5 & =& 2 \times 8 - 3 \times 5 \\
=& 2 \times 8 - 3 \times (13 - 8) & =& 5 \times 8 - 3 \times 13 \\
=& 5 \times (21 - 13) - 3 \times 13 & =& 5 \times 21 - 8 \times 13 \\
=& 5 \times 21 - 8 \times (97 - 4 \times 21) & =& 37 \times 21 - 8 \times 97 \\
=& 37 \times (312 - 3 \times 97) - 8 \times 97 & =& 37 \times 312 - 119 \times 97
\end{aligned}
$$

Therefore, $1 = 37 \times 312 - 119 \times 97$. Equivalently, $s = 37$ and $t = 119$ are the solutions to $312s + 97t = \gcd(312, 97)$.

(d)

$$
\begin{aligned}
312x &\equiv 3 \pmod{97} \\
37 \cdot 312x &\equiv 37 \cdot 3 \pmod{97} \\
x &\equiv 111 \pmod{97} \\
x &\equiv 14 \pmod{97}
\end{aligned}
$$

Q.3

Let $d = \gcd(b + a, b - a)$. By definition, $d \mid (b + a)$ and $d \mid (b - a)$. Therefore, $d \mid (b + a) + (b - a) = 2b$ and $d \mid (b + a) - (b - a) = 2a$. Since $d \mid 2b$ and $d \mid 2a$, $d \mid \gcd(2b, 2a) = 2\gcd(b, a) = 2$.

Hence, $d = 1$ or $d = 2$. Equivalently, we can say that $\gcd(b + a, b - a) \leq 2$.

Q.4

Proof.

For any x, y that $x = y$ and $x, y \in \mathbb{Z}^+$, we can infer that $222 \mid 2^y - 2^x = 0$. $\square$

Q.5

(a)

Yes.

First, we can factorize 561 into $3 \times 11 \times 17$. By Fermat's Little Theorem, we have:

$$
\begin{aligned}
2^2 &\equiv 1 \pmod{3} \\
2^{10} &\equiv 1 \pmod{11} \\
2^{16} &\equiv 1 \pmod{17}
\end{aligned}
$$

Therefore, we can find:

$$
\begin{aligned}
2^{560} &\equiv 2^{2\times 280} \equiv 1 \pmod{3} \\
2^{560} &\equiv 2^{10\times 56} \equiv 1 \pmod{11} \\
2^{560} &\equiv 2^{16\times 35} \equiv 1 \pmod{17}
\end{aligned}
$$

Hence, $2^{560} \equiv 1 \pmod{561}$.

(b)

No.

561 is not a prime number, since $561 = 3 \times 11 \times 17$.

Q.6

Proof.

Sufficient Condition:

Assume, without loss of generality, that $b \geq a$. Let $x = \gcd(a, b)$, $y = \operatorname{lcm}(a, b)$.

By definition, $xy = ab$. Since $x + y = a + b$ and a, b are positive integers, we can infer that:

$$
\begin{aligned}
(x+y)^2 =& (a+b)^2 \\
(x+y)^2 - 4xy =& (a+b)^2 - 4ab \\
(x-y)^2 =& (a-b)^2 \\
y - x =& b - a \\
y - x + x + y =& b - a + a + b \\
2y =& 2b \\
y =& b
\end{aligned}
$$

Therefore, $y = b$ and $x = a$. Since $\gcd(a, b) = a$, we can infer that $a \mid b$.

Necessary Condition:

Assume, without loss of generality, that $b \geq a$.

Since $a \mid b$, it is obvious that $\gcd(a, b) = a$ and $\text{lcm}(a, b) = b$. Therefore, $\gcd(a, b) + \text{lcm}(a, b) = a + b$. □

Q.7

(1)

Proof by Cases.

Case 1: x is an even number.

Since x is an even number, x^2 is also an even number. Therefore, $x^2 - 31$ is an odd number and is not divisible by 36.

Hence, $x^2 \not\equiv 31 \pmod{36}$.

Case 2: x is an odd number.

Let $x = 2k + 1$ where $k \in \mathbb{Z}$. Then, $x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$.

Since 4 is a factor of 36, we can infer that $x^2 \equiv 31 \pmod 4$ should also be true. However, $x^2 \equiv 4k(k + 1) + 1 \equiv 1 \pmod 4$ and $31 \equiv 3 \pmod 4$, which is a contradiction. □

(2)

We can only find two solutions for each of these equations:

$$\begin{cases} x \equiv 14 \text{ or } 17 & \pmod{31} \\ x \equiv 17 \text{ or } 20 & \pmod{37} \end{cases}$$

By Chinese Remainder Theorem, we can find four solutions for this system of linear congruences:

$$x \equiv 17 \text{ or } 572 \text{ or } 575 \text{ or } 1130 \pmod{1147}$$

Q.8

Proof by Contradiction.

Lemma 1. *For any positive integers a, m such that $\gcd(a, m) \neq 1$, there exists a positive integer b where $b \in \mathbb{Z}_m$ such that $ab \equiv 0 \pmod m$.*

Proof.

Let $d = \gcd(a, m)$. By definition, $d \mid a$ and $d \mid m$. Assume that $a = kd$ and $m = ld$ where $k, l \in \mathbb{Z}$. It's obvious that $l \in \mathbb{Z}_m$ and $l \neq 0$, since $l = \frac{m}{d}$ and $d > 1$.

Since $la \equiv lkd \equiv km \equiv 0 \pmod m$, we can infer that $b = l$ is the positive integer we are looking for. □

By the lemma above, we can always find a positive integer b where $b \in \mathbb{Z}_m$ such that $ab \equiv 0 \pmod m$.

If a has an inverse $\bar{a}$ modulo m, then we have:

$$\begin{aligned}
a\bar{a} &\equiv 1 \pmod m \\
ab\bar{a} &\equiv b \pmod m \\
0\bar{a} &\equiv b \pmod m \\
0 &\equiv b \pmod m
\end{aligned}$$

This is a contradiction, since $b \neq 0$ and $b \in \mathbb{Z}_m$. □

Q.9

(a)

$$\begin{aligned}
321 \div 2 =& 160...1 \\
160 \div 2 =& 80...0 \\
80 \div 2 =& 40...0 \\
40 \div 2 =& 20...0 \\
20 \div 2 =& 10...0 \\
10 \div 2 =& 5...0 \\
5 \div 2 =& 2...1 \\
2 \div 2 =& 1...0 \\
1 \div 2 =& 0...1
\end{aligned}$$

Therefore, $321_{10} = 101000001_2$.

(b)

$$\begin{aligned}
1023 =& 2^{10} - 1 \\
=& (10000000000 - 1)_2 \\
=& 1111111111_2
\end{aligned}$$

Therefore, $1023_{10} = 1111111111_2$.

(c)

$$\begin{aligned}
100632 \div 2 =& 50316...0 \\
50316 \div 2 =& 25158...0 \\
25158 \div 2 =& 12579...0 \\
12579 \div 2 =& 6289...1 \\
6289 \div 2 =& 3144...1 \\
3144 \div 2 =& 1572...0 \\
1572 \div 2 =& 786...0 \\
786 \div 2 =& 393...0 \\
393 \div 2 =& 196...1 \\
196 \div 2 =& 98...0 \\
98 \div 2 =& 49...0 \\
49 \div 2 =& 24...1 \\
24 \div 2 =& 12...0 \\
12 \div 2 =& 6...0 \\
6 \div 2 =& 3...0 \\
3 \div 2 =& 1...1 \\
1 \div 2 =& 0...1
\end{aligned}$$

Therefore, $100632_{10} = 11000100100011000_2$.

Q.10

Using Bezout's Theorem, there exists integers s_n, t_n such that:

$$\begin{aligned}
s_1p + t_1q =& \gcd(p, q) = 1 \\
s_2p + t_2r =& \gcd(p, r) = 1 \\
s_3q + t_3r =& \gcd(q, r) = 1
\end{aligned}$$

By multiply these terms together, we have:

$$\begin{aligned}
(s_1p + t_1q)(s_2p + t_2r)(s_3q + t_3r) =& s_1s_2s_3p^2q + s_1s_2t_3p^2r + s_1t_2s_3pqr + s_1t_2t_3pr^2 \\
&+ t_1s_2s_3pq^2 + t_1s_2t_3pqr + t_1t_2s_3q^2r + t_1t_2t_3qr^2 \\
=& (s_1s_2s_3p + t_1s_2s_3q + s_1t_2s_3r + t_1s_2t_3r)pq \\
&+ (t_1t_2s_3q + t_1t_2t_3r)qr + (s_1s_2t_3p + s_1t_2t_3r)rp \\
=& 1
\end{aligned}$$

Therefore, we find $a = s_1s_2s_3p + t_1s_2s_3q + s_1t_2s_3r + t_1s_2t_3r$, $b = t_1t_2s_3q + t_1t_2t_3r$ and $c = s_1s_2t_3p + s_1t_2t_3r$ that satisfy $a(pq) + b(qr) + c(rp) = 1$.

Q.11

By Fermat's Little Theorem, we have $10^{12} \equiv 1 \pmod{13}$. Therefore, we can infer that:

$$10^{100} \equiv 10^{12\times 8+4} \equiv 10^4 \equiv 3 \pmod{13}$$

Since $3^3 \equiv 27 \equiv 1 \pmod{13}$ and $3 \mid 10^{100} - 1$, we can infer that:

$$(10^{100})^{(10^{100})} \equiv 3^{(10^{100})} \equiv 3^1 \equiv 3 \pmod{13}$$

Hence, $(10^{100})^{(10^{100})} \equiv 3 \pmod{13}$.

Q.12

(1)

Proof.

$$\begin{aligned} f(cm) =& c + a_1 cm + a_2 c^2 m^2 + a_3 c^3 m^3 + ... + a_{n-1} c^{n-1} m^{n-1} + c^n m^n \\ =& c(1 + a_1 m + a_2 cm^2 + a_3 c^2 m^3 + ... + a_{n-1} c^{n-2} m^{n-1} + c^{n-1} m^n) \end{aligned}$$

Therefore, $f(cm)$ is a multiple of c. □

(2)

Proof.

We only consider the case when $n = cm$ where $m \in \mathbb{Z}$. Since $f(n)$ grows unboundedly to infinity, we can expect an m_0 that for all $m \geq m_0$, $f(cm) > c$.

From the proof above, we can infer that $f(cm)$ is a multiple of c. Therefore, $\frac{f(cm)}{c}$ is a factor of $f(cm)$ and $\frac{f(cm)}{c} > 1$. Since $f(cm) > c > 1$, $f(cm)$ is a composite number.

We can find infinitely many m that $m \geq m_0$. Therefore, there exists infinitely many $f(cm)$ that is not a prime number. □

(3)

Proof.

From the proof above, we can infer that when $c > 1$, there exists infinitely many n that $f(n)$ is not a prime number. When $c \leq 1$, $f(0) = c \leq 1$ and it will not be a prime number.

In conclusion, non-constant polynomial $f(n)$ cannot generate only prime numbers for all $n \in \mathbb{N}$. □

Q.13

Proof by Contradiction.

By definition, we know $2^{\log_2 3} = 3$.

If $\log_2 3$ is a rational number, then we can write $\log_2 3 = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Since $\log_2 3 > 0$, without loss of generality, we can assume that $a > 0$ and $b > 0$.

Therefore, we have:

$$\begin{aligned} 2^{\frac{a}{b}} &= 3 \\ 2^a &= 3^b \end{aligned}$$

This is a contradiction, since 2^a is an even number and 3^b is an odd number. □

Q.14

Proof.

Assume $\bar{a}_1, \bar{a}_2$ are two inverse of a modulo m. Then, we have:

$$\begin{aligned} \bar{a}_1 a &\equiv 1 \pmod{m} \\ \bar{a}_2 a &\equiv 1 \pmod{m} \\ (\bar{a}_1 - \bar{a}_2) a &\equiv 0 \pmod{m} \end{aligned}$$

Equivalently, we have $m \mid (\bar{a}_1 - \bar{a}_2)a$.

Lemma 2.

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Since a and m are relatively prime and $m \mid (\bar{a}_1 - \bar{a}_2)a$, we can infer that $m \mid (\bar{a}_1 - \bar{a}_2)$. Equivalently, we have $\bar{a}_1 \equiv \bar{a}_2 \pmod{m}$. Hence, the inverse of a modulo m is unique modulo m. □

Q.15

Proof by Contradiction.

Suppose that there are only finitely many primes of the form $4k + 3$ where $k \in \mathbb{N}$. Let them be $q_1, q_2, ..., q_n$. Obviously, $4q_1q_2 \cdots q_n - 1 \equiv -1 \equiv 3 \pmod{4}$

Firstly, 2 is not a factor of $4q_1q_2 \cdots q_n - 1$, since $4q_1q_2 \cdots q_n - 1 \equiv 3 \pmod{4}$, which means it is an odd number.

Secondly, q_i is not a factor of $4q_1q_2 \cdots q_n - 1$, since $4q_1q_2 \cdots q_n - 1 \equiv -1 \pmod{q_i}$ where $i \in \{1, 2, ..., n\}$.

Thirdly, prime factors of $4q_1q_2 \cdots q_n - 1$ cannot all be of the form $4k + 1$, since that:

$$(4k_1 + 1)^{c_1}(4k_2 + 1)^{c_2}(4k_3 + 1)^{c_3} \cdots \equiv 1 \not\equiv 3 \equiv 4q_1q_2 \cdots q_n - 1 \pmod{4}$$

Since all prime number except 2 can be written as $4k + 1$ or $4k + 3$, we can infer that $4q_1q_2 \cdots q_n - 1$ must have a prime factor of the form $4k + 3$ and is not in the list $q_1, q_2, ..., q_n$. □

Q.16

(a)

Using Fermat's Little Theorem, we have:

$$\begin{aligned}
5^{2003} &\equiv 5^{333\times 6+5} \equiv 5^5 \equiv 3 \pmod 7 \\
5^{2003} &\equiv 5^{200\times 10+3} \equiv 5^3 \equiv 4 \pmod{11} \\
5^{2003} &\equiv 5^{166\times 12+11} \equiv 5^{11} \equiv 8 \pmod{13}
\end{aligned}$$

(b)

Using Chinese Remainder Theorem, we can find:

$$\begin{aligned}
M_1 &= 11 \times 13 = 143 \\
M_2 &= 7 \times 13 = 91 \\
M_3 &= 7 \times 11 = 77
\end{aligned}$$

Using Extended Euclidean Algorithm, we can find their inverses:

$$\begin{aligned}
5 \times 143 &\equiv 1 \pmod 7 \\
4 \times 91 &\equiv 1 \pmod{11} \\
12 \times 77 &\equiv 1 \pmod{13}
\end{aligned}$$

Therefore, we have:

$$\begin{aligned}
5^{2003} &\equiv 3 \times 5 \times 143 + 4 \times 4 \times 91 + 8 \times 12 \times 77 \pmod{1001} \\
&\equiv 10993 \pmod{1001} \\
&\equiv 983 \pmod{1001}
\end{aligned}$$

Q.17

Proof.

If $a \equiv b \pmod{m_i}$ for $i = 1, 2, ..., n$ and m_i are pairwise relatively prime, then we have:

$$\begin{aligned}
a &\equiv b \pmod{m_1} \\
a &\equiv b \pmod{m_2} \\
&\ldots \\
a &\equiv b \pmod{m_n}
\end{aligned}$$

By definition, we know that $m_1 \mid (a-b)$, $m_2 \mid (a-b)$, ..., $m_n \mid (a-b)$.

Lemma 3.

If a, b, c are positive integers such that $a \mid c$ and $b \mid c$, then $lcm(a, b) \mid c$.

Proof.

Consider the factorization of a and b, we assume that $a = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$ and $b = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$ where p_i are prime numbers and $c_i, d_i \in \mathbb{Z}$. Without loss of generality, we can assume that $c_i + d_i > 0$ for all i.

For every prime p_i, we can infer that $p_i^{c_i} \mid c$ and $p_i^{d_i} \mid c$. Therefore, $p_i^{\max(c_i,d_i)} \mid c$. By definition, we know that $\mathrm{lcm}(a,b) = p_1^{\max(c_1,d_1)} p_2^{\max(c_2,d_2)} \cdots p_n^{\max(c_n,d_n)} \mid c$. □

By the lemma above, we can infer that $\mathrm{lcm}(m_1, m_2, ..., m_n) \mid (a-b)$. Since $m_1, m_2, ..., m_n$ are pairwise relatively prime, we can infer that $\mathrm{lcm}(m_1, m_2, ..., m_n) = m_1 m_2 \cdots m_n = m$. Therefore, $m \mid (a-b)$. Equivalently, we have $a \equiv b \pmod m$. □

Q.18

Proof.
If there exist a, b that are both solution to a system of linear congruences modulo pair wise relatively prime moduli $m_1, m_2, ..., m_n$, then we have:

$$\begin{aligned} a \equiv b &\equiv c_1 \pmod{m_1} \\ a \equiv b &\equiv c_2 \pmod{m_2} \\ &... \\ a \equiv b &\equiv c_n \pmod{m_n} \end{aligned}$$

By the proof of Q.17, we can infer that $a \equiv b \pmod m$ where $m = m_1 m_2 \cdots m_n$. Equivalently, we say the solution is unique modulo m. □

Q.19

Since these moduli are not pair wise relatively prime, we factorize them into prime numbers. The given conditions can be factorized into:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Using Chinese Remainder Theorem, we can find:

$$\begin{aligned} M_1 &= 3 \times 5 = 15 \\ M_2 &= 2 \times 5 = 10 \\ M_3 &= 2 \times 3 = 6 \end{aligned}$$

Using Extended Euclidean Algorithm, we can find their inverses:

$$\begin{aligned} 1 \times 15 &\equiv 1 \pmod 2 \\ 1 \times 10 &\equiv 1 \pmod 3 \\ 1 \times 6 &\equiv 1 \pmod 5 \end{aligned}$$

Therefore, we have:

$$\begin{aligned} x &\equiv 1 \times 1 \times 15 + 2 \times 1 \times 10 + 3 \times 1 \times 6 && \pmod{30} \\ &\equiv 53 && \pmod{30} \\ &\equiv 23 && \pmod{30} \end{aligned}$$

The solution is of the form $x = 23 + 30k$ where $k \in \mathbb{Z}$.

Q.20

These given conditions can be written as:

$$\begin{aligned} 4 &\equiv (7a + c) \pmod{11} \\ 6 &\equiv (4a + c) \pmod{11} \end{aligned}$$

By subtracting the second equation from the first equation, we have:

$$\begin{aligned} 3a &\equiv -2 && \pmod{11} \\ 4 \cdot 3a &\equiv 4 \cdot -2 && \pmod{11} \\ a &\equiv -8 && \pmod{11} \\ a &\equiv 3 && \pmod{11} \end{aligned}$$

Substitute $a = 3$ into the first equation, we have:

$$\begin{aligned} 21 + c &\equiv 4 && \pmod{11} \\ c &\equiv -17 && \pmod{11} \\ c &\equiv 5 && \pmod{11} \end{aligned}$$

Hence, the next number is $6 \times 3 + 5 \mod 11 = 1$.

Q.21

Proof.

Proof of $\phi(m) \mid \phi(n)$:

Assume the factorization of m is that $m = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$ where p_i are prime numbers and $c_i \in \mathbb{Z}$. Furthermore, we assume the factorization of n is that $n = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n} q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}$ where q_i are prime numbers and $d_i, e_i \in \mathbb{Z}$. Without loss of generality, we can assume that $c_i, d_i, e_i > 0$ for all i and $c_i \leq d_i$.

Since $p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$ is relatively prime to $q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}$, we can infer that:

$$\begin{aligned} \phi(n) =& \phi(p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}) \phi(q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}) \\ =& \phi(p_1^{d_1}) \phi(p_2^{d_2}) \cdots \phi(p_n^{d_n}) \phi(q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}) \end{aligned}$$

Then, for every prime factor p_i of m, we have:

$$\begin{aligned} \phi(p_i^{d_i}) =& p_i^{d_i} - p_i^{d_i - 1} \\ =& (p_i^{c_i} - p_i^{c_i - 1}) p_i^{d_i - c_i} \\ =& \phi(p_i^{c_i}) p_i^{d_i - c_i} \end{aligned}$$

Since $c_i \leq d_i$, we can infer that $p_i^{d_i - c_i} \geq 1$. Therefore, $\phi(p_i^{c_i}) \mid \phi(p_i^{d_i})$. Combining all terms, we have $\phi(m) \mid \phi(n)$.

Proof of $\phi(mn) = m\phi(n)$:
For any prime p and positive integers c, d, we have:

$$\begin{aligned}\phi(p^{c+d}) &= p^{c+d} - p^{c+d-1} \\ &= p^c(p^d - p^{d-1}) \\ &= p^c\phi(p^d)\end{aligned}$$

For $\phi(mn)$, we can infer that:

$$\begin{aligned}\phi(mn) =&\phi(p_1^{c_1+d_1}p_2^{c_2+d_2}\cdots p_n^{c_n+d_n}q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m}) \\ =&\phi(p_1^{c_1+d_1}p_2^{c_2+d_2}\cdots p_n^{c_n+d_n})\phi(q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m}) \\ =&\phi(p_1^{c_1+d_1})\phi(p_2^{c_2+d_2})\cdots\phi(p_n^{c_n+d_n})\phi(q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m}) \\ =&p_1^{c_1}\phi(p_1^{d_1})p_2^{c_2}\phi(p_2^{d_2})\cdots p_n^{c_n}\phi(p_n^{d_n})\phi(q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m}) \\ =&[p_1^{c_1}p_2^{c_2}\cdots p_n^{c_n}][\phi(p_1^{d_1})\phi(p_2^{d_2})\cdots\phi(p_n^{d_n})\phi(q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m})] \\ =&m\phi(n)\end{aligned}$$

Therefore, $\phi(mn) = m\phi(n)$. ☐

Q.22

Proof.
Since we know $n = pq$ and the value of $(p-1)(q-1)$, then we can find $p+q$ by solving the following equation:

$$\begin{aligned}(p-1)(q-1) =&pq - p - q + 1 \\ (p-1)(q-1) =&pq - (p+q) + 1 \\ p + q =&pq - (p-1)(q-1) + 1\end{aligned}$$

Let $s = p + q$, then we have:

$$\begin{aligned}p^2 - ps + pq =&p^2 - p(p+q) + pq \\ =&p^2 - p^2 - pq + pq \\ =&0\end{aligned}$$

Therefore, p is a root of the equation $p^2 - ps + pq = 0$. Then we can find p by solving the quadratic equation. Equivalently, we have:

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

Then, we can find q by $q = \frac{n}{p}$.
This equation always has two real roots, this is because:

$$\begin{aligned}s^2 - 4n =&(p+q)^2 - 4pq \\ =&p^2 + 2pq + q^2 - 4pq \\ =&p^2 - 2pq + q^2 \\ =&(p-q)^2 \\ \geq&0\end{aligned}$$

And both roots are always positive, since:

$$s - \sqrt{s^2 - 4n} = \sqrt{s^2} - \sqrt{s^2 - 4n} > 0$$

□

Q.23

(a)

$$\hat{M} = M^e \bmod n = 8^7 \bmod 65 = 57$$

(b)

Since $n = 65 = 5 \times 13$, we can find $p = 5$ and $q = 13$. Then, we can find $\phi(n) = (p-1)(q-1) = 4 \times 12 = 48$.

The private key d then will be the inverse of e modulo $\phi(n)$. Using Extended Euclidean Algorithm, we can find $7 \times 7 \equiv 1 \pmod{48}$. Therefore, $d = 7$.

(c)

$$M = \hat{M}^d \bmod n = 57^7 \bmod 65 = 8$$

Q.24

Proof by Cases.

Since $(p-1)(q-1) = \gcd(p-1, q-1) \cdot \operatorname{lcm}(p-1, q-1)$, we can infer that $\lambda(n) \mid \phi(n)$. By definition, $\gcd(e, \phi(n)) = 1$, and then we know $\gcd(e, \lambda(n)) = 1$. Hence, we can always find d' such that $ed' \equiv 1 \pmod{\lambda(n)}$.

Case 1: $\gcd(M, n) = 1$

Since $ed' \equiv 1 \pmod{\lambda(n)}$, we can assume that $ed' - 1 = k\lambda(n)$ where $k \in \mathbb{Z}$. Also, we can assume $\lambda(n) = t(p-1) = s(q-1)$ where $t, s \in \mathbb{Z}$. Then, we have:

$$\begin{aligned}
C^{d'} &\equiv M^{ed'} && \pmod{p} \\
&\equiv M^{k\lambda(n)} \cdot M && \pmod{p} \\
&\equiv M^{kt(p-1)} \cdot M && \pmod{p} \\
&\equiv (M^{p-1})^{kt} \cdot M && \pmod{p}
\end{aligned}$$

Since $\gcd(M, n) = 1$ and $n = pq$, we know that $\gcd(M, p) = 1$. By Fermat's Little Theorem, we know that $M^{p-1} \equiv 1 \pmod{p}$. Therefore, we have:

$$\begin{aligned}
C^{d'} &\equiv (M^{p-1})^{kt} \cdot M && \pmod{p} \\
&\equiv 1^{kt} \cdot M && \pmod{p} \\
&\equiv M && \pmod{p}
\end{aligned}$$

Similarly, we can infer that $C^{d'} \equiv M \pmod{q}$. Since p and q are relatively prime, we can infer that $C^{d'} \equiv M \pmod{n}$.

Case 2: $\gcd(M, n) = p$

To proof $C^{d'} \equiv M^{ed'} \equiv M \pmod{n}$ is equivalent to proof $n \mid M(M^{ed'-1} - 1)$. Since $p \mid M$ and $n = pq$, we only need to proof $q \mid M^{ed'-1} - 1$. Equivalently, we need to proof $M^{ed'-1} \equiv 1 \pmod{q}$.

Since $ed' \equiv 1 \pmod{\lambda(n)}$, we can assume that $ed' - 1 = k\lambda(n)$ where $k \in \mathbb{Z}$. Also, we can assume $\lambda(n) = t(p-1) = s(q-1)$ where $t, s \in \mathbb{Z}$. Then, we have:

$$\begin{aligned} M^{ed'-1} &\equiv M^{k\lambda(n)} &\pmod{q} \\ &\equiv M^{ks(q-1)} &\pmod{q} \\ &\equiv (M^{q-1})^{ks} &\pmod{q} \end{aligned}$$

Since $\gcd(M, n) = p$ and $n = pq$, we know that $\gcd(M, q) = 1$ still holds. By Fermat's Little Theorem, we know that $M^{q-1} \equiv 1 \pmod{q}$.

$$\begin{aligned} M^{ed'-1} &\equiv (M^{q-1})^{ks} &\pmod{q} \\ &\equiv 1^{ks} &\pmod{q} \\ &\equiv 1 &\pmod{q} \end{aligned}$$

Hence, $C^{d'} \equiv M \pmod{n}$.

Case 3: $\gcd(M, n) = q$

Similar to Case 2, we can proof $C^{d'} \equiv M \pmod{n}$.

Case 4: $\gcd(M, n) = n$

Since $0 \leq M < n$, we can infer that $M = 0$. Therefore, $C^{d'} \equiv M^{ed'} \equiv 0 \equiv M \pmod{n}$. $\square$