# VE203 Assignment 7

Name: YIN Guoxin   Student ID: 517370910043

**Q1.** Since $ac \equiv bc \pmod{m}$, we have $m|(ac-bc)$. Since $\frac{m}{\gcd(c,m)}|m$, we also have $\frac{m}{\gcd(c,m)}|(ac-bc) = (a-b)c$ and also $\gcd(\frac{m}{\gcd(c,m)}, c) = 1$. From this, we know that $\gcd(c,m)|(a-b)$, which means $a \equiv b \left(\bmod \frac{m}{\gcd(c,m)}\right)$.

**Q2.** Since $36x \equiv 75(\bmod 1309)$, we have $1309|(36x-75)$, i.e. there exists $m \in \mathbb{Z}$ such that $75 = 36x+1209m$. Since

$$\begin{aligned}
1309 &= 36 \times 36 + 13 \\
36 &= 2 \times 13 + 10 \\
13 &= 10 + 3 \\
10 &= 3 \times 3 + 1 \\
3 &= 3 \times 1,
\end{aligned}$$

we know that gcd(1309,36)=1. Therefore, there we have

$$\begin{aligned}
1 &= 10 - 3 \times 3 \\
&= 10 - 3 \times (13 - 10) \\
&= 4 \times 10 - 3 \times 13 \\
&= 4 \times (36 - 2 \times 13) - 3 \times 13 \\
&= 4 \times 36 - 11 \times 13 \\
&= 4 \times 36 - 11 \times (1309 - 36 \times 36) \\
&= 400 \times 36 - 11 \times 1309,
\end{aligned}$$

which means $1 = 400 \times 36 - 11 \times 1309$. Therefore $75 = 400 \times 75 \times 36 - 11 \times 75 \times 1309 = 30000 \times 36 - 825 \times 1309$. Hence, $x = 30000$ is a solution.

**Q3.** To solve this system, we need to solve

$$\begin{aligned}
x &\equiv 2(\bmod 5) \\
x &\equiv 4(\bmod 7) \\
x &\equiv 4(\bmod 13)
\end{aligned}$$

Now,

$$\begin{aligned}
m &= m_1 m_2 m_3 = 455 \\
M_1 &= \frac{455}{5} = 91 \\
M_2 &= \frac{455}{7} = 65 \\
M_3 &= \frac{455}{13} = 35
\end{aligned}$$

To find $y_1$,

$$\begin{aligned}
91 &= 18 \times 5 + 1 \\
1 &= 91 - 18 \times 5
\end{aligned}$$

Hence, let $y_1 = 1$. To find $y_2$,

$$\begin{aligned}
65 &= 9 \times 7 + 2 \\
7 &= 3 \times 2 + 1 \\
1 &= 7 - 3 \times 2 \\
&= 7 - 3 \times (65 - 9 \times 7) \\
&= 28 \times 7 - 3 \times 65
\end{aligned}$$

Hence, let $y_2 = -3$. To find $y_3$,

$$\begin{aligned}
35 &= 2 \times 13 + 9 \\
13 &= 9 + 4 \\
9 &= 2 \times 4 + 1 \\
1 &= 9 - 2 \times 4 \\
&= 9 - 2 \times (13 - 9) \\
&= 3 \times 9 - 2 \times 13 \\
&= 3 \times (35 - 2 \times 13) - 2 \times 13 \\
&= 3 \times 35 - 8 \times 13
\end{aligned}$$

Hence, let $y_3 = 3$. Therefore,

$$x = \sum_{k=1}^{n} a_k M_k y_k = 2 \times 91 \times 1 + 4 \times 65 \times (-3) + 4 \times 35 \times 3 = -178(\mathrm{mod} 455).$$

Therefore, the solutions are -178+455$y$, where $y \in \mathbb{Z}$.

**Q4.**

$$\begin{aligned}
6|(x-5) \Rightarrow & 3|(x-2) \\
& 2|(x-1), \\
10|(x-3) \Rightarrow & 5|(x-3) \\
& 2|(x-1), \\
15|x-8) \Rightarrow & 5|(x-3) \\
& 3|(x-2)
\end{aligned}$$

Since there are no contradiction between the equations in the right hand side, there must exist solutions and we turn the system into

$$\begin{aligned}
x &\equiv 1 (\text{mod } 2) \\
x &\equiv 2 (\text{mod } 3) \\
x &\equiv 3 (\text{mod } 5)
\end{aligned}$$

Now,

$$\begin{aligned}
m &= m_1 m_2 m_3 = 30 \\
M_1 &= \frac{30}{2} = 15 \\
M_2 &= \frac{30}{3} = 10 \\
M_3 &= \frac{30}{5} = 6
\end{aligned}$$

To find $y_1$,

$$\begin{aligned} 15 &= 7 \times 2 + 1 \\ 1 &= 15 - 7 \times 2 \end{aligned}$$

Hence, let $y_1 = 1$. To find $y_2$,

$$\begin{aligned} 10 &= 3 \times 3 + 1 \\ 1 &= 10 - 3 \times 3 \end{aligned}$$

Hence, let $y_2 = 1$. To find $y_3$,

$$\begin{aligned} 6 &= 5 + 1 \\ 1 &= 6 - 5 \end{aligned}$$

Hence, let $y_3 = 1$. Therefore,

$$x = \sum_{k=1}^{n} a_k M_k y_k = 1 \times 15 \times 1 + 2 \times 10 \times 1 + 3 \times 6 \times 1 = 53(\mathrm{mod} 30).$$

Therefore, the solutions are $53{+}30y$, where $y \in \mathbb{Z}$.

**Q5.** Now,

$$\begin{aligned} m &= m_1 m_2 m_3 m_4 = 6545 \\ M_1 &= \frac{6545}{5} = 1309 \\ M_2 &= \frac{6545}{7} = 935 \\ M_3 &= \frac{6545}{11} = 595 \\ M_4 &= \frac{6545}{17} = 385 \end{aligned}$$

To find $y_1$,

$$\begin{aligned} 1309 &= 261 \times 5 + 4 \\ 5 &= 4 + 1 \\ 1 &= 5 - 4 \\ &= 5 - (1309 - 261 \times 5) \\ &= 262 \times 5 - 1309 \end{aligned}$$

Hence, let $y_1 = -1$. To find $y_2$,

$$\begin{aligned} 935 &= 133 \times 7 + 4 \\ 7 &= 4 + 3 \\ 4 &= 3 + 1 \\ 1 &= 4 - 3 \\ &= 4 - (7 - 4) \\ &= 2 \times 4 - 7 \\ &= 2 \times (935 - 133 \times 7) - 7 \\ &= 2 \times 935 - 267 \times 7 \end{aligned}$$

Hence, let $y_2 = 2$. To find $y_3$,

$$\begin{aligned} 595 &= 11 \times 54 + 1 \\ 1 &= 595 - 11 \times 54 \end{aligned}$$

Hence, let $y_3 = 1$. To find $y_4$,

$$\begin{aligned} 385 &= 22 \times 17 + 11 \\ 17 &= 11 + 6 \\ 11 &= 6 + 5 \\ 6 &= 5 + 1 \\ 1 &= 6 - 5 \\ &= 6 - (11 - 6) \\ &= 2 \times 6 - 11 \\ &= 2 \times (17 - 11) - 11 \\ &= 2 \times 17 - 3 \times (385 - 22 \times 17) \\ &= 68 \times 17 - 3 \times 385 \end{aligned}$$

Hence, let $y_4 = -3$. Therefore,

$$x = \sum_{k=1}^{n} a_k M_k y_k = 5 \times 1309 \times (-1) + 3 \times 935 \times 2 + 8 \times 595 \times 1 + 2 \times 385 \times -3 = 1515 (\text{mod } 6545).$$

Therefore, the solutions are 1515+6545$y$, where $y \in \mathbb{Z}$.

**Q6.** Suppose, for a contradiction, that there exists $M, C \in \mathbb{N}$ such that for all $n > M$, $n \log_2(n) \leq C \log_2(n)$. But it cannot be true since when $n > C$, $n \log_2(n) > C \log_2(n)$ always hold.

**Q7.** We just need to prove that $\log_a(n) = O \log_b(n)$ where $a, b$ are positive integers greater than 1. Then,

$$\lim_{n \to \infty} \frac{\log_a(n)}{\log_b(n)} = \lim_{n \to \infty} \frac{\frac{1}{n(\ln a)}}{\frac{1}{n(\ln b)}} = \frac{\ln b}{\ln a},$$

which means $\log_a(n) = O \log_b(n)$. When $a = 2, b = 10$, $a = 2, b = e$, $a = 10, b = 2$, $a = 10, b = e$, $a = e, b = 2$, $a = e, b = 10$, we can see that they have the same order from the equation we proved.

**Q8.** For all $x \in \mathbb{R}$, $\lfloor x^3 - 4 \rfloor \leq x^3 - 4$. For $x \leq 2$, $|\lfloor x^3 - 4 \rfloor| \leq |x^3 - 4| < |x^3 + 4| = |x^3(1 + \frac{4}{x^3})| \leq |x^3(1 + 4)| = |(x^3)| \times 5$. Therefore, by choosing $C \in \mathbb{N}$ with $C \geq 5$, we can see that $\lfloor x^3 - 4 \rfloor$ is $O(x^3)$. Conversely, $\lfloor x^3 - 4 \rfloor \geq x^3 - 5$. It is clear that for all $\epsilon > 0$, there exists $D \in \mathbb{R}$ with $D > 0$ such that for all $x > D$,

$$|1 - \frac{5}{x^3}| \geq 1 - \epsilon$$

So, choosing $\epsilon = \frac{1}{2}$, we get $D \in \mathbb{R}$ with $D > 0$ such that for all $x > D$,

$$|1 - \tfrac{5}{x^3}| \geq \tfrac{1}{2} \text{ and } |\lfloor x^3 - 4 \rfloor| > |x^3 - 5| = x^3 |1 - \tfrac{5}{x^3}| \geq \tfrac{1}{2} x^3$$

So, if $C \in \mathbb{N}$ is such that $C \geq 2$, then $|x^3| \leq 2 \times |\lfloor x^3 - 4 \rfloor|$, which shows that $x^3$ is $O(\lfloor x^3 - 4 \rfloor)$.

Therefore, they have the same order.

**Q9.** No. For $n$ large enough,

$$\lim_{n \to \infty} \frac{n^n}{n^{n-k}} = \lim_{n \to \infty} n^k \to \infty,$$

So there doesn't exist $C \in \mathbb{R}$ with $C \geq 0$ such that $\lim_{n \to \infty} \frac{n^n}{n^{n-k}} = C$, which means $n^n \neq O(n^{n-k})$.

**Q10.**

(i) Note that the summation only makes sense when $n \geq 2$, therefore, we only discuss conditions when $n \geq 2$.

- When $n = 2$, $\sum_{j=2}^{2} \frac{1}{j} = \frac{1}{2}$ and $\int_1^2 \frac{1}{x}dx = \ln x|_1^2 = \ln 2 - \ln 1 = \ln 2 > \frac{1}{2}$.
- If $n > 2$ and $\sum_{j=2}^{n} \frac{1}{j} < \int_1^n \frac{1}{x}dx$ holds, suppose for $n+1$, $\sum_{j=2}^{n+1} \frac{1}{j} = \sum_{j=2}^{n} \frac{1}{j} + \frac{1}{n+1} < \int_1^n \frac{1}{x}dx + \frac{1}{n+1}$. Besides, $\int_1^{n+1} \frac{1}{x}dx = \int_1^n \frac{1}{x}dx + \int_n^{n+1} \frac{1}{x}dx = \int_1^n \frac{1}{x}dx + \ln x|_n^{n+1} = \int_1^n \frac{1}{x}dx + \ln(n+1) - ln(n) > \int_1^n \frac{1}{x}dx + \frac{1}{n+1}$. Therefore, we have $\sum_{j=2}^{n+1} \frac{1}{j} < \int_1^{n+1} \frac{1}{x}dx$.

(ii) $H(n) = \sum_{k=0}^{n-1} \frac{1}{n-k} = \sum_{j=1}^{n} \frac{1}{j} = 1 + \sum_{j=2}^{n} \frac{1}{j} < 1 + \int_1^n \frac{1}{x}dx < 1 + \ln n$. So, when $n > e$, $\ln e > 1$, $1 + \ln e < 2\ln n$. Therefore, we have when $n > e$, $H(n) < 2\ln n$, which means $O(\ln(n))$.

**Q11.**

(i) The pseudocode is as follow,

```
Input: a_1, ..., a_n, n unsorted elements
Output: all the a_i, 1 ≤ i ≤ n in increasing order
for k → 2 to n do
    i ← 1
    j ← k − 1
    while i < j do
        m ← ⌊(i + j)/2⌋;
        if a_k > a_m then
            i ← m + 1;
        else
            j ← m
    p ← a_k;
    for l ← 0 to k − i − 1 do
        a_{k−l} ← a_{k−l−1};
    a_i ← p
return (a_1, ..., a_n) in increasing order.
```

(ii)
- Insertion Sort Algorithm: 8+(1+2)+(1+3)+(4+1)+(1+5)+(4+3)+(3+5)+(2+7)=50
- Binary Insertion Sort Algorithm: 8+(1+3)+(3+4)+(3+2)+(5+6)+(5+4)+(5+6)+(7+8)=70

(iii) We define a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ that on input $n$ counts the worst-case number of comparisons needed sort a list of length $n$. For a specific $j^{th}$ element to sort, if there is $k$ comparisons during the **while** loop, which means $i = k - 1$, there will be $j - i - 1 + 1 + 1 = j - i + 1 = j - k + 1$ comparisons during the inner **for** loop. So there are $k + j - k + 1 = j + 1$ comparisons in total during the $j^{th}$ passes. Adding all $j$ we get

$$\sum_{j=2}^{n}(j+1) = \frac{n^2}{2} + \frac{3n}{2} - 2$$

Besides, we also have $n$ comparisons for the outer for loops, so the total number of comparisons is $f(n) = n + \frac{n^2}{2} + \frac{3n}{2} - 2 = \frac{n^2}{2} + \frac{5n}{2} - 2$. Since it is a polynomial of degree 2, $f(n) = O(n^2)$.

(iv) We define a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ that on input $n$ counts the worst-case number of comparisons (excluded comparisons in while loop and for loop) needed sort a list of length $n$. For a specific $k^{th}$ element to sort, the worst case for the while-loop is $2^q = k - 1$, $q = \log_2(k-1)$. Because there are $N$ elements in the list, the complexity is $O(n \log_2 n)$.

Since we know for insertion sort, the corresponding complexity is $O(n^2)$. Since $O(n \log_2 n)$ is way smaller than $O(n^2)$, the Binary Insertion Sort Algorithm is significantly faster than Insertion Sort.