離散數學 107-2

Homework 04

姓名: 葉子瑄。學號: 107590041

截止收件: 2019.05.08 (Wednesday) 23:59 pm (week-12)

Homework 04 題目

(Prob. 1) page 259, chapter 4.1 Exercise 30

(Prob. 2) page 269, chapter 4.2 Exercise 4

(Prob. 3) page 290, chapter 4.3 Exercise 40(c)

(Prob. 4) page 301, chapter 4.4 Exercise 6(b)

(Prob. 5) page 301, chapter 4.4 Exercise 20

(Prob. 6) page 308, chapter 4.5 Exercise 2

(Prob. 7) page 323, chapter 4.6 Example 26

注意事項

(a) 要熟悉 LaTeX 請翻閱 lshort。

(b) 記得在最後一頁，回報完成作業小時數 (估算，取整數)。

(c) 將檔案夾命名為 hw04_107590xxx，將檔案夾壓縮成 hw04_107590xxx.zip，上傳到網路學園。

(d) LaTeX 數學符號請查此表: List of LaTeX mathematical symbols。

(e) 作業抄襲，以零分計。作業提供給他人抄襲，以零分計。

(f) 作業遲交一週內成績打五折，作業遲交超過一週以零分計。

Problem 01 (4.1 Exercise 30)

(a) $-3 \equiv 43 \pmod{23}$

(b) $-12 \equiv 17 \pmod{29}$

(c) $94 \equiv -11 \pmod{21}$

Problem 02 (4.2 Exercise 4)

(a) 27

(b) 693

(c) 958

(d) 31775

Problem 03 (4.3 Exercise 40(c))

(a) The steps used by the Euclidean algorithm to find $\gcd(35, 78)$ are

$$\begin{aligned} 78 &= 2 \cdot 35 + 8 \\ 35 &= 4 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

(b) Then we need to work our way back up

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\ &= 3 \cdot (35 - 4 \cdot 8) - 8 = 3 \cdot 35 - 13 \cdot 8 \\ &= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) = 29 \cdot 35 - 13 \cdot 78 \end{aligned}$$

Problem 04 (4.4 Example 6(b))

(a) First we go through the Euclidean algorithm computation that $gcd(34, 89) = 1$:

$$\begin{aligned}
89 &= 2 \cdot 34 + 21 \\
34 &= 1 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

(b) Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3{-}2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34
\end{aligned}$$

Thus s = -34, so an inverse of 34 modulo 89 is -34, which can also be written as 55.

Problem 05 (4.4 Exercises 20)

The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$.

$a_1 = 2, m_1 = 3$
$a_2 = 1, m_2 = 4$
$a_3 = 3, m_3 = 5$

$m = m_1 \cdot m_2 \cdot m_3 = 60$
$M_1 = 60/3 = 20$
$M_2 = 60/4 = 15$
$M_3 = 60/5 = 12$

Then we need to find inverses y_i of M_i modulo m_i
$y_1 = 2$
$y_2 = 3$
$y_3 = 3$
$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 233 \equiv 53 \pmod{60}$
So the solutions are all integers of the form $53 + 60k$, where k is an integer.

Problem 06 (4.5 Exercises 2)

(a) 58

(b) 60

(c) 52

(d) 3

Problem 7 (4.6 Exercises 22)

First we
find $d = 2753$, the inverse of $e = 17$ *modulo* $52 \cdot 60$.

Next we compute $c^d \pmod{n}$ for each of the four given numbers:
$3185^{2753} \pmod{3233} = 1816$ (which are the letters SQ),
$2038^{2753} \pmod{3233} = 2008$ (which are the letters UI),
$2460^{2753} \pmod{3233} = 1717$ (which are the letters RR), and
$2550^{2753} \pmod{3233} = 0411$ (which are the letters EL).

The message is SQUIRREL.

完成作業小時數

完成作業小時數:共 3 小時(估算，取整數)