離散數學 HW04

易頡 110054809
隨班附讀

1 QUESTION

- page 259, chapter 4.1 Exercise 30
- page 269, chapter 4.2 Exercise 4
- page 290, chapter 4.3 Exercise 40(c)
- page 301, chapter 4.4 Exercise 6(b)
- page 301, chapter 4.4 Exercise 20
- page 308, chapter 4.5 Exercise 2
- page 323, chapter 4.6 Example 26

2 ANSWER

2.1 page 259, chapter 4.1 Exercise 30

Find the integer a such that
(a) $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$.
(b) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$.
(c) $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$.

(a) $a = 43 - 46 = -3$
(b) $a = 17 - 29 = -12$
(c) $a = -11 + 21 \times 5 = 94$

2.2 page 269, chapter 4.2 Exercise 4

Convert the binary expansion of each of these integers to a decimal expansion.
(a) $(1\ 1011)_2$
(b) $(10\ 1011\ 0101)_2$
(c) $(11\ 1011\ 1110)_2$
(d) $(111\ 1100\ 0001\ 1111)_2$

(a) 27
(b) $693 = 2^0 + 2^2 + 2^4 + 2^5 + 2^7 + 2^9$
(c) $958 = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9$
(d) $31775 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^{10} + 2^{11} + 2^{12} + 2^{13} + 2^{14}$

2.3 page 290, chapter 4.3 Exercise 40(c)

Using the method followed in Example 17, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

$$35, 78$$

The calculation of the greatest common divisor takes several steps:

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

Then we need to work our way back up

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

2.4 page 301, chapter 4.4 Exercise 6(b)

Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

$$a = 34, m = 89$$

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

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

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

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

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

2.5 page 301, chapter 4.4 Exercise 20

Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences x ≡ 2 (mod 3), x ≡ 1 (mod 4), and x ≡ 3 (mod 5).

The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$.
$a_1 = 2, m_1 = 3$
$a_2 = 1, m_2 = 4$
$a_3 = 3, m_3 = 5$

$m = m_1 \cdot m_2 \cdot m_3 = 60$
$M_1 =$ $m/3 = 20$, $M_2 =$ $m/4 = 15$, $M_3 =$ $m/5 = 12$
Then we need to find inverses y_i of M_i modulo m_i
$y_1 =$ 2 , $y_2 =$ 3 , $y_3 =$ 3
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 =$ $80 + 45 + 108 = 233$ $\equiv$ 53 (mod 60)
So the solutions are all integers of the form $53 + 60k$, where k is an integer.

2.6 page 308, chapter 4.5 Exercise 2

Which memory locations are assigned by the hashing function h(k) = k **mod** 101 to the records of insurance company customers with these Social Security numbers?

(a) 104578690
(b) 432222187
(c) 372201919
(d) 501338753

(a) 58
(b) 60
(c) 52
(d) 3

2.7 page 323, chapter 4.6 Example 26

What is the original message encrypted using the RSA system with n = 53 · 61 and e = 17 if the encrypted message is 3185 2038 2460 2550? (To decrypt, first find the decryption exponent d, which is the inverse of e = 17 modulo 52 · 60.)

First we find, the inverse of $e = 17$ *modulo* $52 \cdot 60$.
A computer algebra system tells us that $d =$ 2753 .
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 .