Contents

1 Section 4.1

1.1 Theorem 1

Proof:

$$a|b \implies b = a \cdot m$$
$$a|c \implies c = a \cdot n$$

For some $m, n \in \mathbb{Z} \implies m+n \in \mathbb{Z}$. Then $b+c = am+an = a(m+n) \therefore a|b+c$.

1.2 Division Algorithm

The function **div** is called the division algorithm.

$$\text{div}(a, d) = a \text{ div } d = \left\lfloor \frac{a}{d} \right\rfloor \tag{1}$$
$$\text{div} : \mathbb{Z} \times \mathbb{Z}^{+} \implies \mathbb{Z} \tag{2}$$

The function receives a dividend and divisor and produces the quotient.

1.3 Modulus Algorithm

The function **mod** is called the modulus algorithm.

$$\text{mod}(a, d) = a \text{ mod } d = a - \left\lfloor \frac{a}{d} \right\rfloor \tag{3}$$

where $a = d \cdot q + r$.

$$\text{mod} : \mathbb{Z} \times \mathbb{Z}^{+} \implies \mathbb{Z} \tag{4}$$

The function receives a dividend and divisor and produces the remainder.

$$a \equiv b \pmod{m} \iff m | (a - b) \tag{5}$$

1.4 Remarks

1.
$$\mathbb{Z}_m \, (Z \text{ mod } m)$$
$$Z_m = \{0_m, 1_m, 2_m, \cdots, (m-1)_m\}$$

   where 0_m is a set

   - $r \in 0_m$ if $r \equiv 0 \pmod{m}$
   - $r \in 1_m$ if $r \equiv 1 \pmod{m}$

2 Section 4.2

2.1 Theorem 1

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \tag{6}$$

where k is a nonnegative integer, $a_0, a_1, \cdots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

2.2 Example

When $b = 10, a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$$7254887 = 7 \cdot 10^6 + 2 \cdot 10^5 + 5 \cdot 10^4 + 4 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$$

3 Section 4.3

3.1 Prime Factorization

$$\begin{aligned}
24 &= 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1 \cdot 5^0 \\
36 &= 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \cdot 5^0 \\
60 &= 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3^1 \cdot 5^1
\end{aligned}$$

$$\begin{aligned}
\mathrm{gcd} &= 2^{\min} \cdot 3^{\min} \cdot 5^{\min} \\
\mathrm{gcd} &= 2^2 \cdot 3^1 \cdot 5^0
\end{aligned}$$

3.2 Greatest Common Divisor

$d = \mathrm{gcd}(a, b)$ if $d \geq x$ for all x such that $x \mid a \& x \mid b$.

3.3 Least Common Multiple

$m = \mathrm{lcm}(a, b)$ if $m \leq y$ for all y such that $a \mid y \& b \mid y$.

3.4 Example 4.3.9

$x = -1$ is a solution to $x^m + 1 = 0$ if m is odd.

$$\begin{aligned}
x^m + 1 &= (x + 1)\left(x^{m-1} - x^{m-2} + x^{m-3} - x^{m-4} + \cdots - x + 1\right) \\
a^m + 1 &= (a + 1)\left(a^{m-1} - a^{m-2} + \cdots - a + 1\right)
\end{aligned}$$

$$\begin{aligned}
a \text{ is great than } 1 &\implies a + 1 > 1 \\
x \text{ is at least } 3 &\implies a + 1 < a^m + 1
\end{aligned}$$

$\therefore 1 < a + 1 < a^m + 1$

3.5 4.3.40

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.

a)

b)

c)

d)

e)

f)

g) 2002, 2339

(a) Show that $\gcd(x, y) = 1$.

(b) Find $x, y, \in \mathbb{Z}$, such that $2002x + 2339y = 1$.

- By the Euclidean Algorithm

$$
\begin{aligned}
2339 &= 2002 \cdot 1 + 337 \\
2002 &= 337 \cdot 6 + 317 \\
337 &= 317 \cdot 1 + 20 \\
317 &= 20 \cdot 15 + 17 \\
20 &= 17 \cdot 1 + 3 \\
17 &= 3 \cdot 5 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (16 - 3 \cdot 5) \\
&= 3 \cdot 6 - 17 \\
&= (20 - 17 \cdot 1) \cdot 6 + (-1) \cdot 17 \\
&= 20 \cdot 6 + (-7) \cdot 17 \\
&= 20 \cdot 6 + (-7)(317 - 20 \cot 15) \\
&= 20 \cdot 111 + (-7) \cdot 317 \\
&= (337 - 317 \cdot 10) \cdot 111 + (-7) \cdot 317 \\
&= 317 \cdot 111 + (-118) \cdot 317 \\
&= 317 \cdot 111 + (-118)(2002 - 337 \cdot 6) \\
&= 317 \cdot 819 + (-118) \cdot 2002 \\
&= (2339 - 2002 \cdot 1) \cdot 819 + (-118) \cdot 2002 \\
&= 2339 \cdot 819 + (-937) \cdot 2002 \\
x &= -937, y = 819
\end{aligned}
$$

h)

i)

4 Section 4.4

4.1 Theorem 1

$$\begin{aligned} ax + b &= c \\ a^{-1} \cdot ax &= c - b \cdot a^{-1} \\ x &= (c - b) \cdot a^{-1} \end{aligned}$$

$$\begin{aligned} 4x + 2 &\equiv 1 (\text{mod } 9) \\ 4x &\equiv -1 (\text{mod } 9) \\ 4x &\equiv 8 (\text{mod } 9) \\ 7 \cdot (4x &\equiv 8 (\text{mod } 9)) \\ x &\equiv 56 (\text{mod } 9) \\ x &\equiv 2 (\text{mod } 9) \end{aligned}$$

4.2 Chinese Remainder Theorem

$$\begin{aligned} x &\equiv a_1 (\text{mod } m_1) \\ x &\equiv a_2 (\text{mod } m_2) \\ x &\equiv a_3 (\text{mod } m_3) \end{aligned}$$

Where x is the same and mod m_i is pair-wise relatively prime.

Let $m = m_1, m_2, \cdots m_n$

$$M_i = \frac{m}{m_i} \tag{7}$$

y_i as inverse of $M_i \text{mod } m_i$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \tag{8}$$

4.2.1 Example

$$\begin{aligned} x &\equiv 1 (\text{mod } 5) \\ x &\equiv 2 (\text{mod } 7) \\ x &\equiv 3 (\text{mod } 4) \end{aligned}$$

$$\begin{aligned} m &= 5 \cdot 7 \cdot 4 = 140 \\ M_1 &= \frac{140}{5} = 28 \\ M_2 &= \frac{140}{7} = 20 \\ M_2 &= \frac{140}{4} = 35 \end{aligned}$$

$$
\begin{aligned}
y_1 \cdot 28 &= 1(\text{mod } 5) = 2 \\
y_2 \cdot 20 &= 1(\text{mod } 7) = 6 \\
y_3 \cdot 35 &= 1(\text{mod } 4) = 3
\end{aligned}
$$

$$
\begin{aligned}
x &= 1 \cdot 28 \cdot 2 + 2 \cdot 20 \cdot 6 + 3 \cdot 35 \cdot 3 \\
&= 611 = 51(\text{mod } 140)
\end{aligned}
$$

4.3 Method of Back Substitution

$$
\begin{aligned}
x &\equiv 1(\text{mod } 5) \\
x &\equiv 2(\text{mod } 7) \\
x &\equiv 3(\text{mod } 4)
\end{aligned}
$$

$$
\begin{aligned}
x &\equiv 1(\text{mod } 5) \\
\implies x &= 5t + 1
\end{aligned}
$$

Then $x \equiv 2(\text{mod } 7)$ becomes

$$
\begin{aligned}
5t + 1 &\equiv 2(\text{mod } 7) \\
3 \cdot 5t &\equiv 1(\text{mod } 7) \cdot 3 \\
t &\equiv 3(\text{mod } 7) \\
\implies \qquad t &= 7s + 3 \\
\implies \qquad c &= 5(7s + 3) + 1 \\
&= 355 + 16
\end{aligned}
$$

Then $x \equiv 3(\text{mod } 4)$ becomes

$$
\begin{aligned}
355 + 16 &\equiv 3(\text{mod } 4) \\
355 &\equiv 3(\text{mod } 4) \\
35 &\equiv 3(\text{mod } 4) \\
s &\equiv 9(\text{mod } 4) \\
s &\equiv 1(\text{mod } 4) \\
s &= 4r + 1 \\
x &= 35(4r + 1) + 16 = 140r + 51
\end{aligned}
$$

4.4 Fermat's Little Theorem

4.4.1 Example

$$
\begin{aligned}
a &= 7 \\
p &= 13 \implies p - 1 = 12 \\
121 &= 12 \cdot 10 + 1
\end{aligned}
$$

$$
7^{p-1} \equiv 1 \text{mod } 13
$$

$$
\begin{aligned}
&7^{121} \bmod 13 \\
&\equiv 7^{12 \cdot 10+1} \bmod 13 \\
&\equiv 7^{12 \cdot 10} \cdot 7 \bmod 13 \\
&\equiv \left(7^{p-1}\right)^{10} \cdot 7 \bmod 13 \\
&\equiv 1^{10} \cdot 7 \bmod 13 \\
&= 7 \bmod 13
\end{aligned}
$$