Modular Exponentiation

Monday, January 31, 2022 12:44 PM

Recall : Modular Arithmetic

Missing: #2, 9, 26

§4.2. Integer Representation and Algorithms

1] Thrm : (the base-b expansion of n)

If $n \in \mathbb{Z}^n$, then n can be expressed uniquely as

$$n = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0$$

where $0 \leq a_i < b$, $a_k \neq 0$, $k \geq 0$

2] Binary Expansion : $b = 2$

e.g. $(1011)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1$

$= 11$

3] Hexadecimal Expansion : $b = 16$

using 0–9, A—F for 0–15

e.g. $2AF = 2 \cdot 16^2 + 10 \cdot 16^1 + 15 = 687$

4] e.g. Convert 165 to binary

$$\begin{aligned}
165 &= 2 \cdot 82 + \underline{1} \\
82 &= 2 \cdot 41 + \underline{0} \\
41 &= 2 \cdot 20 + \underline{1} \\
20 &= 2 \cdot 10 + \underline{0} \\
10 &= 2 \cdot 5 + \underline{0} \\
5 &= 2 \cdot 2 + \underline{1} \\
2 &= 2 \cdot 1 + \underline{0} \\
1 &= 2 \cdot 0 + \underline{1}
\end{aligned}$$

$(10100101)_2 = 165$

5] Binary - Hex conversion

$(0000)_2 = 0, \quad (0001)_2 = 1, \quad \dots, \quad (1111)_2 = 15 = F$

e.g. $\underbrace{1010}_{A}\ \underbrace{0101}_{5} = (A5)_{16}$

6] Adding: (in base b)

in base 2

$$\begin{array}{r} 10101 \\ 11101 \\ \hline 110010 \end{array}$$

in base 16

$$\begin{array}{r} 9AFE \\ A03 \\ \hline A501 \end{array}$$

7] Multiplication (in base b)

$$\begin{array}{r} 10101 \\ 1001 \\ \hline 10101 \\ 10101000 \\ \hline 10111101 \end{array}$$

8] Modular Exponentiation:

To find $b^n \pmod m$

let $n = (a_{k-1}\ a_{k-2}\ \dots\ a_1\ a_0)_2$

i

$x = 1; \quad p = b \pmod m$

for $i = 0$ to $k-1$ do

{ if $a_i = 1$ then

$x = x * p \pmod m;$

$(19)_2 = 10011$

$3^{19} = 3^{16} \cdot 3^2 \cdot 3^1$

$3 \longrightarrow x = 3$

$3^2 = 9 \longrightarrow x* = 3^2$

$9^2 = 3^4$

3^8

$3^{16} \longrightarrow x* = 3^{16}$

$x = x * p \pmod{m}$;

$p = p * p \pmod{m}$

}

Return x;

e.g. Compute $3^{19} \pmod{11}$

a_i	x: 1	p: 3
1	3	9
1	$27 \equiv 5$	$9^2 \equiv 4$
0	5	$16 \equiv 5$
0	5	$25 \equiv 3$
1	$15 \equiv 4$	9

$$3^{19} \equiv 4 \pmod{11}$$

9] Exer:

① $1370 \bmod 6$

$\equiv 137 \times 10$

$\equiv 5 * 4$

$\equiv 20 \equiv 2 \pmod{6}$

② $1372 \bmod 3$

$\equiv 1371 + 1$

$\equiv 0 + 1$

$\equiv 1 \pmod{3}$

③ $513720 \pmod{7}$

10] Divisibility tricks

① by 3: add the digits

$$1372 = 1 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 2$$

$$\equiv 1(1^3) + 3(1^2) + 7(1) + 2 \pmod 3$$
$$\equiv 1 + 3 + 7 + 2$$
$$\equiv 13 \equiv 1 \pmod 3$$

② by 4 : take the last 2 digits

$$51733 = 51700 + 33$$
$$\equiv 0 + 33 \pmod 4$$
$$\equiv \underline{1} \pmod 4$$

③ by 5 : take the last digit

④ by 9 :

$$1372 = 1 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 2$$
$$\equiv 1(1^3) + 3(1^2) + 7(1) + 2 \pmod 9$$
$$\equiv 1 + 3 + 7 + 2$$
$$\equiv 13 \equiv 4 \pmod 9$$

⑤ by 11 : alternating +/− from R to Left.

$$\overleftarrow{-+-+}$$
$$1372 = 1 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 2$$
$$\equiv 1(-1)^3 + 3(-1)^2 + 7(-1)^1 + 2 \pmod{11}$$
$$\equiv -1 + 3 - 7 + 2$$
$$\equiv -3 \equiv 8 \pmod{11}$$

⑥ by 7 : HW