Integer Algorithms

Monday, April 6, 2026 11:24 AM

Recall: Integer Representation

Missing:
700# 6, 17, 28
800# 18
+B# 709, 720 (mod)
Ex# 825 on 1/28, 2/9

1) Addition in base b

$b = 2$

$$\begin{array}{rl} 5 & \longrightarrow \quad 0\ 1\ 0\ 1 \\ +\ b & \longrightarrow \quad 0\ 1\ 1\ 0 \\ \hline & 1\ 0\ 1\ 1 \longrightarrow 11 \end{array}$$

$b = 16$

$$\begin{array}{r} 9\ A\ F\ E \\ A\ 0\ 3\ + \\ \hline A\ 5\ 0\ 1 \end{array}$$

2) Multiplication in base b (e.g. $b = 2$)

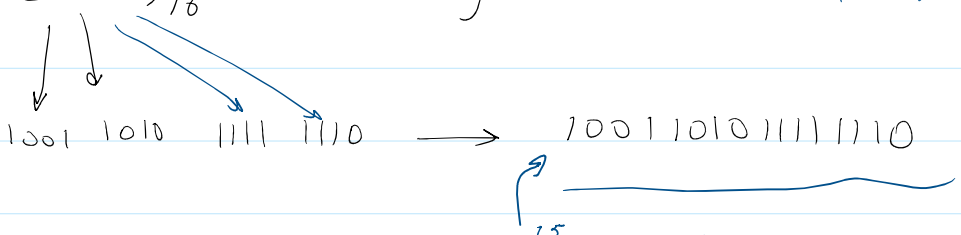
$$\begin{array}{rl} 6 & \longrightarrow \quad 1\ 1\ 0 \\ 5 & \longrightarrow \quad 1\ 0\ 1 \\ \hline & 1\ 1\ 0 \\ & 0 \quad + \\ & 1\ 1\ 0 \\ \hline & 1\ 1\ 1\ 1\ 0 \\ & 16\ 8\ 4\ 2 \longrightarrow 30 \end{array}$$

3) Ex (base-conversion)

① convert $(9AFE)_{16}$ to decimal.

$9AFE = 9 \times 16^3 + 10 \cdot 16^2 + 15 \cdot 16 + 14 =$

② Convert $(9AFE)_{16}$ to binary



③ Convert 165 to hex

$165 = 10 \cdot 16 + 5$

$10 = 0 \cdot 16 + 10$

$(A5)_{16}$

④ Convert 165 to Oct (base 8)

$165 = (A5)_{16} \rightarrow 1010\ 0101$

$= (245)_8$

4] Modular Exponentiation (§ 4.2)

To compute $b^n \bmod m$

Alg. ModExp (b, n , m)

Return $b^n \pmod m$

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

let $x = 1$, $p = b \pmod m$

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

{ if $a_i == 1$ then

$x = x * p \pmod m$;

$p = p * p \pmod m$;

}

$3^{19} \bmod 11$

$19 = (10011)_2$

$3^1 \rightarrow 3$

$\downarrow$ ^2

$3^2 \rightarrow 3^2$

$\downarrow$

3^4

$\downarrow$

3^8

$\downarrow$

$3^{16} \rightarrow 3^{16}$

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

Return x;

5] e.g. Compute $3^{19} \bmod 11$ using ModExp.

$19 = (10011)_2$

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

$\Longrightarrow \quad x = 4$

```
if a_i == 1 then
    x = x * p (mod m);
p = p * p (mod m);
```

6] Euclidean Algorithm (§ 4.3)

To find gcd (a, b)

Thrm: $\gcd(a, b) = \gcd(b, a \bmod b)$

e.g. Find gcd (252 198)

$252 = \underline{1} \cdot 198 + \underline{54}$

$198 = \underline{3} \cdot 54 + \underline{36}$

$54 = \underline{1} \cdot 36 + \underline{18}$

$36 = \underline{2} \cdot 18 + \underline{0}$ ← gcd = 18

7] Exer: gcd (156, 69)

Soln.

$$156 = 2 \cdot 69 + 18$$
$$69 = 3 \cdot 18 + 15$$
$$18 = 1 \cdot 15 + 3 \leftarrow \text{gcd}$$
$$15 = 5 \cdot 3 + 0$$