Integers & Algorithms

- Representations in different bases
- Base conversion
- Algorithms for integer operations

base 10 – everyday use
binary (2)
octal / hexadecimal
(8) (16)

Thm Let $b \in \mathbb{Z}_{>1}$, $n \in \mathbb{Z}_+$. n can be represented uniquely in the form:

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

$k \in \mathbb{Z}_{\geq 0}$

$0 \leq a_i < b$ for each $i = 0, \ldots, k$ and $a_k \neq 0$

$\Rightarrow b$ is the base of the representation

$\Rightarrow a_0 = n \bmod b$

"base b expansion of n" $(a_k a_{k-1} \ldots a_1 a_0)_b$

ex: $(10110)_2$ decimal expansion

$$= 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$$

$$= 2 + 4 + 16 = 22$$

ex: $(43B)_{16}$ decimal expansion (10)

0	1	2	…	9	A	B	C	D	E	F
					10	11	12	13	14	15

$$11 + \underset{48}{3 \cdot 16} + 4 \cdot 16^2 = 1083$$

binary expansion

$$(\underbrace{100}_{4}\,\underbrace{0011}_{3}\,\underbrace{1011}_{B})_2$$

Base conversion

an algorithm for constructing base b expansion of an integer n

$$n = b \cdot q_0 + a_0 \qquad a_0 < b$$

$$q_0 = b \cdot q_1 + a_1$$

continue till the quotient is 0

$$(a_k \, a_{k-1} \, \ldots \, a_0)_b$$

$$q_{k-1} = b \cdot 0 + a_k$$

ex 1083 what is the octal expansion of 1083

8

$$\begin{array}{r|l} 1083 & 8 \\ \hline -8 & 135 \\ 28 & \\ 24 & \\ 43 & \\ \hline 3 & \end{array}$$

$$\begin{array}{r|l} 135 & 8 \\ \hline 8 & 16 \\ 55 & \\ 48 & \\ \hline 7 & \end{array}$$

$$1083 = 8 \cdot \underbrace{135}_{q_0} + \underbrace{3}_{a_0}$$

$$135 = 8 \cdot \underbrace{16}_{q_1} + \underbrace{7}_{a_1}$$

$$16 = 8 \cdot 2 + \underbrace{0}_{a_2}$$

$$2 = 8 \cdot 0 + \underbrace{2}_{a_3}$$

$$\Rightarrow (2073)_8$$

ex Binary expansion of 13

$$13 = 2 \cdot 6 + 1$$
$$6 = 2 \cdot 3 + 0$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

$$(1101)_2$$

Algorithms for integer operations

$a = (a_{n-1}\ a_{n-2}\ \cdots\ a_1\ a_0)_2$

$b = (b_{n-1}\ b_{n-2}\ \cdots\ b_1\ b_0)_2$ } n bit representation

$5 \Rightarrow (\underbrace{0000\ 0101}_{8 \text{ bit representation.}})_2$

addition

$c_i, s_i \in \{0, 1\}$

$a_0 + b_0 = \underbrace{c_0}_{\text{carry bit}} \cdot 2 + \underbrace{s_0}_{\text{right most digit}}$

```
  1001
  1011
+
 10100   c0 = 1
         c1 = 1
```

$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$

$s_n\ s_{n-1}\ \cdots\ s_1\ s_0$ } $a+b$

sum (a, b)
$c = 0$
for $i = 0$ to $n-1$
  $d = \lfloor (a_i + b_i + c)/2 \rfloor$ ← bit operation
  $s_j = (a_i + b_i + c) - 2d$ ←
  $c = d$
end
$s_n = d$

$O(n)$ $O(n^2)$
$\Omega(n)$ $\Omega(1)$
$\Theta(n)$

multiplication

$a = (a_{n-1}\ a_{n-2}\ \cdots\ a_1\ a_0) = 2^{n-1} a_{n-1} + 2^{n-2} a_{n-2} + \cdots + a_0$

$b = (b_{n-1}\ \cdots\ b_1) = 2^{n-1} b_{n-1} + 2^{n-2} b_{n-2} + \cdots + b_0$

$a \cdot b = a \cdot (2^{n-1} b_{n-1} + \cdots + b_0)$

$$a \cdot 2^J b_J = \begin{cases} 0 & b_J = 0 \\ 2^J \cdot a & b_J = 1 \end{cases}$$

shift a to left J places

multiply (a, b)

$p = 0$

for $j = 0$ to $n-1$

if $b_j == 1$

c = a shifted j places

$p = p + c$ } $O(n)$

end

end

return p

how many shifts ?

how many bit operations?

$\underbrace{0 \quad 1 \quad 2 \quad \ldots\ldots \quad n-1}_{n^2}$

$O(n^2)$ shifts

$O(n^2)$ bit operations from summation

Modular Exponentiation

⇒ How to efficiently compute $b^n \bmod m$?

$$\Rightarrow \quad a_{n-1} 2^{n-1} + a_{n-2} 2^{n-2} + \ldots + a_0$$

$$(a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \ldots + a_0) \bmod m$$

$$((a_{n-1} \bmod m)(b^{n-1} \bmod m) + \ldots + (a_0 \bmod m)) \bmod m$$

$a_i < b$

$$\leadsto \quad xy \bmod m = (x \bmod m)(y \bmod m) \bmod m$$

$$5^{26} \bmod 11$$

$26 = 2^4 + 2^3 + 2^1$

$$= 5^{16} \cdot 5^8 \cdot 5^2 \bmod 11$$

$$= 5^{2^4} \cdot 5^{2^3} \cdot 5^{2^1} \bmod 11$$

$(10^{26} \cdot 8 + \ldots)$

$5^{26} \cdot 2^{26}$

$5^2 \cdot 5^{24} \bmod 11$

3

$= 3 \cdot 5^2 \cdot 5^{22} \bmod 11$

3

$= (\underbrace{5^{2^4} \bmod 11}_{5})(\underbrace{5^{2^3} \bmod 11}_{4})(\underbrace{5^{2^1}}_{3} \bmod 11)$

$= 5 \cdot 4 \cdot 3 \bmod 11$

$= 5$

$5^{2^3} = (\underbrace{5^2 \cdot 5^2}_{(5^{2^2})^2})(5^2 \cdot 5^2)$

$5^1 \bmod 11 = 5$

$5^2 \bmod 11 = 3$

$5^{2^2} \bmod 11 = 9$

$= (5^2 \bmod 11)(5^2 \bmod 11)$

$(5^{2^3} \bmod 11) =$

$(5^{2^2})(5^{2^2}) \bmod 11$

$= 4$

$5^{2^4} \bmod 11 = 5$

$b^n \bmod m$, $n = a_{k-1} 2^{k-1} + a_{k-2} 2^{k-2} + \dots + a_0$

modular exponentiation ($b^n \bmod m$)

```
x = 1
p = b mod m
for i = 0 to k-1
    if a_i = 1 then x = (x.p) mod m
    p = (p.p) mod m
return x
```