Integers and Algorithms

Dr. Kahrobaei
City Tech (CUNY)
Representation of Integers

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

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

Where $k$ is a nonegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than $b$, and $a_k \neq 0$. 
Binary expansions

Choosing 2 as the base gives binary expansions of integers. In binary notation each digit is either a 0 or a 1.

Example: What is the decimal expansion of the integer that has \((1\ 0101\ 1111)_2\) as its binary expansion?

\[
(1\ 0101\ 1111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0
\]
Hexadecimal Expansions

Sixteen is another base used in computer science. The base 16 expansion of an integer is called its hexadecimal expansion. The hexadecimal digits used are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F where the letter A through F represent the digits corresponding to the numbers 10 through 15 (in decimal notation).
Hexadecimal Expansions

Example

Example: What is the decimal expansion of the hexadecimal expansion of \((2AE0B)_{16}\) ?

Solution:

\[
(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = (175627)_{10}
\]

Each hexadecimal digit can be represented using four bits. \((1110\ 0101)_{2} = (E5)_{16}\) because \((1110)_{2} = (E)_{16}\) and \((0101)_{2} = (5)_{16}\)

Bytes, which are bit strings of length eight, can be represented by two hexadecimal digits.
Algorithm: Constructing Base b Expansions

Procedure $base \, b \, expansion(n: \text{positive integer})$

$q := n$
$k := 0$

While $q \neq 0$

begin

\[ a_k := q \mod b \]
\[ q := \left\lfloor \frac{q}{b} \right\rfloor \]
\[ k := k+1 \]

end \{the \, base \, b \, expansion \, of \, n \, is \, (a_{k-1} \, ... \, a_1 \, a_0)_b \} \}
Find the binary expansion of \((241)_{10}\)

\[ \begin{align*}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &= 2 \cdot 7 + 1 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 2 \cdot 1 + 1 \\
1 &= 2 \cdot 0 + 1 \\
\end{align*} \]

\((241)_{10} = (1111\ 0001)_{2}\)
Algorithm Addition of Integers

**Procedure** $add(a, b$: positive integers$)$

{the binary expansions of $a$ and $b$ are $(a_{n-1} a_{n-2} \ldots a_1 a_0)_2$ and $(b_{n-1} b_{n-2} \ldots b_1 b_0)_2$, respectively}$

c:=0

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

begin

  $d:=\lfloor (a_j + b_j +c)/2 \rfloor$
  
  $s_j := a_j + b_j +c -2d$

  $c:=d$

end

$s_n :=c$

{the binary expansion of the sum is $(s_n s_{n-1} \ldots s_1 s_0)_2$}
Algorithm Multiplying Integers

Procedure multiply(a, b: positive integers)
{the binary expansions of a and b are \((a_{n-1} a_{n-2} \ldots a_1 a_0)_2\) and \((b_{n-1} b_{n-2} \ldots b_1 b_0)_2\), respectively}
for \(j:=0\) to \(n-1\)
begin
    if \(b_j = 1\) then \(c_j := a \text{ shifted } j \text{ places}\)
    else \(c_j := 0\)
end
\{\(c_0, c_1, \ldots, c_{n-1}\) are partial products\}
p:=0
For \(j:=0\) to \(n-1\)
    \(p := p + c_j\)
\{\(p\) is the value of \(ab\)\}
Algorithm Computing div and mod

**Procedure** division algorithm(*a*: integer,  *b*: positive integer)

q:=0
r:=|a|
While r >=d
Begin
  r:=r-d
  q:=q+1
End
If a<0 and r>0 then
Begin
  r:=d-r
  q:=(q+1)
End

{q=a div d is the quotient, r=a mod d is the remainder}
Algorithm Modular Exponentiation

procedure modular exponentiation (b: integer, \( n = (a_{k-1} a_{k-2} \ldots a_1 a_0) \mod m \), m: positive integers)

\( x := 1 \)

\( \text{power} := b \mod m \)

for \( i := 0 \) to \( k-1 \)

begin

\( \text{if } a_i = 1 \text{ then } x := (x \cdot \text{Power}) \mod m \)

\( \text{power} := (\text{power.power}) \mod m \)

end

\{x equals \( b^n \mod m \}\)
The Euclidean Algorithm

**Lemma:** is $a = bq + r$ where $a$, $b$, $q$ and $r$ are integers. Then $\gcd(a, b) = \gcd(b, r)$

**Algorithm The Euclidean Algorithm**

**Procedure** $\gcd(a, b : \text{positive integers})$

1. $x := a$
2. $y := b$
3. While $y \neq 0$
4. Begin
5. $r := x \mod y$
6. $x := y$
7. $y := r$
8. End
9. $\{ \gcd(a,b) \text{ is } x \}$
Example

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.
Successive uses of the division algorithm give:

\[ 662 = 414 \cdot 1 + 248 \]
\[ 414 = 248 \cdot 1 + 166 \]
\[ 248 = 166 \cdot 1 + 82 \]
\[ 166 = 82 \cdot 2 + 2 \]
\[ 82 = 2 \cdot 41 \]