NUMBER THEORY

Lecture 15

DIVISIBILITY AND MODULAR ARITHMETIC

INTRODUCTION

- Division of an integer by a positive integer produces a quotient and a remainder.
- Working with these remainders leads to modular arithmetic.
- Modular Arithmetic plays important role in math and CS.
- Applications of Modular Arithmetic includes generating pseudorandom numbers, assigning computer memory locations to files, constructing check digits and encrypting messages.

DIVISION

Definition: If a and b are integers with $a \neq 0$, then a *divides* b if there is an integer c such that $b = ac$ (or equivalent if b/a is an integer).

- When a divides b we say that a is a *factor or divisor* of b, and that b is a *multiple* of a.
- The notation $a \mid b$ denotes that a divides b.
- If a | b, then b/a is an integer.
- If a does not divide b, we write $a \nmid b$.

Theorem 1: Let a, b, and c be integers, where $a \neq 0$. Then

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

ii. If $a \mid b$, then $a \mid bc$ for all integers c;

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

DIVISION ALGORITHM

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

In the equality given above, d is *divisor*, a is *dividend*, q is *quotient*, r is *remainder*.

This notion is used to express the quotient and remainder:

$$q = a\ \textbf{\textit{div}}\ d$$
$$r = a\ \textbf{\textit{mod}}\ d$$

div and mod
$q = a$ div d
$r = a$ mod d

Remark: Note that both *a div d* and *a mod d* for a fixed d are functions on the set of integers. Furthermore, when a is an integer and d is a positive integer, we have $a\ \textbf{\textit{div}}\ d = \left\lfloor \frac{a}{d} \right\rfloor$ and $a\ \textbf{\textit{mod}}\ d = a - d$.

INTEGER REPRESENTATION AND ALGORITHMS

BASE B REPRESENTATIONS

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

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

where k is a nonnegative integer, $a_0, a_1, \dots a_k$ are nonnegative integers less than b, and $a_k \neq 0$. The a_j, $j = 0, \dots, k$ are called the base-b digits of the representation.

- The representation of n given in Theorem 1 is called the base b expansion of n and is denoted by $(a_k a_{k-1} \dots a_1 a_0)_b$.
- We usually omit the subscript 10 for base 10 expansions.

ALGORITHM: CONSTRUCTING BASE B EXPANSIONS

```
procedure base b expansion(n, b: positive integers with b > 1)
q := n
k := 0
while (q ≠ 0)
      a_k := q mod b
      q := q div b
      k := k + 1
return(a_{k-1} ,…, a_1,a_0){(a_{k-1} … a_1a_0)_b is base b expansion of n}
```

- q represents the quotient obtained by successive divisions by b, starting with $q = n$.
- The digits in the base b expansion are the remainders of the division given by q mod b.
- The algorithm terminates when $q = 0$ is reached.

COMPARISON OF HEXADECIMAL, OCTAL, AND BINARY REPRESENTATIONS

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Initial 0s are not shown

Each octal digit corresponds to a block of 3 binary digits.
Each hexadecimal digit corresponds to a block of 4 binary digits.
So, conversion between binary, octal, and hexadecimal is easy.

OCTAL EXPANSIONS

The octal expansion (base 8) uses the digits $\{0,1,2,3,4,5,6,7\}$.

Example: What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$

Example: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

HEXADECIMAL EXPANSIONS

The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. The hexadecimal system uses the digits {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}. The letters A through F represent the decimal numbers 10 through 15.

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

Solution:

$$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$$

Example: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Solution: $14\cdot16^1 + 5\cdot16^0 = 224 + 5 = 229$

BASE CONVERSION

- To construct the base b expansion of an integer n:
  - Divide n by b to obtain a quotient and remainder.
    - $n = bq_0 + a_0 \quad 0 \leq a_0 \leq b$
  - The remainder, a_0 , is the rightmost digit in the base b expansion of n. Next, divide q_0 by b.
    - $q_0 = bq_1 + a_1 \quad 0 \leq a_1 \leq b$
  - The remainder, a_1, is the second digit from the right in the base b expansion of n.
  - Continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder. The process terminates when the quotient is 0.

CONVERSION BETWEEN BINARY, OCTAL, AND HEXADECIMAL EXPANSIONS

Example: Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.

Solution:

- To convert to octal, we group the digits into blocks of three $(011\ 111\ 010\ 111\ 100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,7,2,7, and 4. Hence, the solution is $(37274)_8$.
- To convert to hexadecimal, we group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,E,B, and C. Hence, the solution is $(3EBC)_{16}$.

CONVERSION EXAMPLE

Example:

Convert n=122 to base b=3:

- 122÷3=40 remainder 2
- 40÷3=13 remainder 1
- 13÷3=4 remainder 1
- 4÷3=1 remainder 1
- 1÷3=0 remainder 1

- **Answer:** 122 base 10=11112 base 3

BASE CONVERSION

Example: Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

The remainders are the digits from right to left yielding $(30071)_8$.