3.6 Integers and Algorithms

Representation of Integers:

Thm 1 $b \in \mathbb{Z}^+$, $b > 1$, $n \in \mathbb{Z}^+$. n can be expressed as

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \qquad k \in \mathbb{W},$$

$$a_i \in \mathbb{W} \ \forall i = 0, \ldots, k, \quad a_i < b, \quad a_k \neq 0.$$

This is basically just expanded form of a # in some base b.

Ex 1 Convert from decimal to binary numbers.

(a) 231

(b) 4532

Ex 2 Convert these integers from binary to decimal.

(a) 1011101101

3.6 (cont)

Ex 2 (cont)

(b) 11 1011 1110

Ex 3 Convert $(BADFACED)_{16}$ to binary. from hexadecimal

Note: hexadecimal uses 16 digits:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9,

A, B, C, D, E, F

(A = 10, B = 11, C = 13 etc. in base 10 #s)

★ see table pg 222

Lemma 1 Let $a = bq + r$, $a, b, q, r \in \mathbb{Z}$.

Then $\gcd(a, b) = \gcd(b, r)$

Pf ① Suppose $d \mid a$ and $d \mid b$, i.e. d is a common divisor of a and b. $\Rightarrow d \mid (a - bq) \Leftrightarrow d \mid r$

$\Rightarrow$ any common divisor of a and b is also a divisor of b and r.

3.6 (cont)

② (other case) Suppose $d|b$ and $d|r$. (finish)

Euclidean Algorithm

$a, b \in \mathbb{Z}^+$, $a \geq b$.

$$a = bq_1 + r_2 \qquad 0 \leq r_2 < b$$

$$b = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4 \qquad 0 \leq r_4 < r_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

(eventually a remainder of zero occurs)

$$\Rightarrow \gcd(a,b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{n-1}, r_n)$$
$$= \gcd(r_n, 0) = r_n$$

Ex 4 Find $\gcd(12, 18)$ using Euclidean algorithm.

3.6 (cont)

Ex 5 Find gcd.

(a) gcd(1000, 5040)

(b) gcd(11111, 111111)

(c) gcd(12345, 54321)

3.6 (cont)

Ex 6 Perform arithmetic operations (in base 2).

(a) $1111_2 \times 10011_2$

(b) $11101_2 + 1010110_2$

(c) $111001_2 - 10011_2$