1 4.2 (cont.)

$1011011_2 = 133_8 = 5B_{16}$

(convert in blocks of 3 bits for octal, and in blocks of 4 bits for hexadecimal)

Example: Convert 241_{10} to binary.

241 div 2 = 120, remainder 1

120 div 2 = 60, remainder 0

60 div 2 = 30, remainder 0

30 div 2 = 15, remainder 0

15 div 2 = 7, remainder 1

7 div 2 = 3, remainder 1

3 div 2 = 1, remainder 1

1 div 2 = 0, remainder 1

Read from bottom to top: 11110001_2

2 4.3: Primes, GCD, LCM

Prime: integer greater than 1 that is divisible by only 1 and itself

Every positive integer > 1 is divisible at least by 1 and itself.

Composite: positive integer > 1 that is not prime.

Integer n is composite $\iff \exists a \in \mathbb{Z}$ s.t. $a|n$ and $1 < a < n$

Fundamental Theorem of Arithmetic: every positive integer > 1 can be written uniquely as a prime number or as the product of two or more primes, where the prime factors are written in non-decreasing order.

Examples: $100 = 2 \cdot 2 \cdot 5 \cdot 5$, $641 = 641$, $999 = 3^3 \cdot 37$

Longer example: 7007

$2|7007$ fails

$3|7007$ fails

$5|7007$ fails

$7|7007$ works: $7007/7 = 1001$

$7|1001$ works: $1001/7 = 143$

$7|143$ fails

$11|143$ works: $11/143 = 13$

$7007 = 7 \cdot 7 \cdot 11 \cdot 13$

The factorization can be optimized, for example, by only verifying for primes up to the square root of the original number.

Greatest Common Divisor (GCD)

gcd(36, 24) = 12

$36 = 2^2 \cdot 3^2$, $24 = 2^3 \cdot 3^1$

What 36 and 24 have in common at most, prime by prime, is $2^2 \cdot 3^1 = 12$ (minimized exponents).

$\gcd(2^{13} \cdot 3^5 \cdot 7^1 \cdot 13^2,\ 2^2 \cdot 3^1 \cdot 11^5) = 2^2 \cdot 3^1$

Co-prime or relatively prime

Example: $11^2 \cdot 13^5$ and $3^2 \cdot 5^3$. The gcd is 1.

Least Common Multiple (LCM)

$\mathrm{lcm}(2^{13} \cdot 3^5 \cdot 7^1 \cdot 13^2, 2^2 \cdot 3^1 \cdot 11^5) = 2^{13} \cdot 3^5 \cdot 7^1 \cdot 11^5 \cdot 13^2$

$\mathrm{lcm}(120,\ 500) = \mathrm{lcm}(2^3 \cdot 3 \cdot 5,\ 2^2 \cdot 5^3) = 2^3 \cdot 3^1 \cdot 5^3 = 3000$

gcd(630, 196)

630 mod 196 = 42

gcd(196, 42)

196 mod 42 = 28

gcd(42, 28)

42 mod 28 = 14

gcd(28, 14)

28 mod 14 = 0

gcd(14,0)

So gcd(630, 196) = 14