# Primes

1/25/12

Note Title

**Definition**: Let P be a positive integer greater than 1.
p is a prime number if the only positive factors of p are 1 and p.
p is a composite number if it has a positive factor other than 1 and itself.

$p = 5$ factors 1 & 5 prime

$p = 6$ factors 1, 2, 3, 6 Composite

$p = 1$ is neither a prime nor a composite #

First 10 prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Primes are the building blocks of positive integers.

**Theorem 1. Fundamental Theorem of Arithmetic**

Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.

Every natural number greater than 1 can be written as a product involving only prime factors.

**Examples**

$100 = 4 \times 25 = 2 \times 2 \times 5 \times 5 = 2^2 \cdot 5^2$

$1024 = \underbrace{2 \times 2 \times \cdots \times 2}_{(10 \text{ times})} = 2^{10}$

**Theorem 2.** If $n$ is a composite integer, then $n$ has a prime factor less than or equal to $\sqrt{n}$.

**Examples** Find the prime factorizations of (a) 101 and (b) 7007.

(a) 101 $\quad \sqrt{101} = 10...$ Primes < 10 are 2, 3, 5, 7,

$$2 \overline{)101}\ \ 50, \quad 100,\ 1$$

3|101 ? NO $\quad$ 5|101 ? NO $\quad$ 7|101 ? NO

101 is a prime #

(b) 7007

2|7007 ? NO

3|7007 ? NO

5|7007 ? NO

7|7007 ? Yes

$7007 = 7 \times \underline{1001}$

7|1001 ? Yes

$1001 = 7 \times 143$

$7007 = 7 \times 7 \times 143$

$= 7 \times 7 \times 11 \times 13$

$7007 = 7^2 \cdot 11 \cdot 13$

$$7 \overline{)1001} = 143: \quad 7,\ 30,\ 28,\ 21,\ 21,\ 0$$

7|143 ? NO

11|143 ? Yes

$143 = 11 \times 13$

**Theorems 3&4.** There are infinitely many primes.

The number of primes not exceeding $x$ approaches $\frac{x}{\ln(x)}$ as $x \to \infty$.

**Mersenne primes** have the form $2^p - 1$, where $p$ is a prime

$2^3 - 1 = 7 \qquad 2^5 - 1 = 31 \qquad 2^{11} - 1 = 2047 = 23 * 89$

**Greatest Common Divisor (GCD)**

**Definition**: Let $a$ and $b$ be nonzero integers.
The largest positive integer $d$ such that $d | a$ and $d | b$ is called the greatest common divisor of $a$ and $b$, and is denoted by $\gcd(a, b)$.

If $\gcd(a, b) = 1$, then $a$ and $b$ are relatively prime.

**Example** Find $\gcd(24, 36)$, $\gcd(15, 22)$.

$\gcd(24, 36)$

$24 = 2 \times \underline{12}$

$36 = 3 \times \underline{12}$

$\gcd(24, 36) = 12$

$\gcd(15, 22)$

$15 = 3 \times 5$

$22 = 2 \times 11$

$\gcd(15, 22) = 1$

15 & 22 are relatively prime.

**Definition**: Integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$, where $1 \le i, j \le n$ and $i \ne j$.

Problem 17 b. $14, 15, 21$ $\gcd(15, 21) = 3$

Section 4.3

$\gcd(14, 15) = 1$ $\gcd(14, 21) = 7$

$\therefore$ 14, 15, 21 are not pairwise relatively prime

**Least Common Multiple (LCM)**

The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by lcm(a,b).

**Example:** Find lcm(24,36) and lcm(15,22).

$lcm(24,36) = 2^3 \times 3^2 = 8 \times 9 = 72$

$24 = 2 \times 12 = 2 \times 2 \times 6$

$= 2 \times 2 \times 2 \times 3 = 2^3 \times 3$

$36 = 2 \times 18 = 2 \times 2 \times 9$

$= 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$

$lcm(15,22) = 2 \times 3 \times 5 \times 11$

$= 330$

$15 = 3 \times 5$

$22 = 2 \times 11$

If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$,

$$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots p_n^{\min(a_n,b_n)}$$

$$lcm(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots p_n^{\max(a_n,b_n)}$$

**Example:** $24 = 2 \times 12 = 2^3 \cdot 3^1$ $\quad 36 = 3 \times 12 = 2^2 \cdot 3^2$

$gcd(24,36) = 2^{\min(3,2)} \cdot 3^{\min(1,2)} = 2^2 \cdot 3^1 = 12$

$lcm(24,36) = 2^{\max(3,2)} \cdot 3^{\max(1,2)} = 2^3 \cdot 3^2 = 8 \cdot 9 = 72$

**Theorem 5**. Let a and b be positive integers. Then ab = gcd(a,b)*lcm(a,b).

**Euclidean Algorithm**

Let $a = qb + r$, where $a, b, q, r$ are integers, $0 \le r < |b|$.

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

```
function gcd(a,b)
  x := a
  y := b
  while y≠0
   begin
      r := x mod y
      x := y
      y := r
   end
   return x
```

Find $\gcd(414, 662)$ $\qquad 414 = 0 \cdot 662 + 414$

$= \gcd(662, 414)$ $\qquad 662 = 1 \cdot 414 + 248$

$= \gcd(414, 248)$ $\qquad 414 = 1 \cdot 248 + 166$

$= \gcd(248, 166)$ $\qquad 248 = 1 \cdot 166 + 82$

$= \gcd(166, 82)$ $\qquad 166 = 2 \cdot 82 + 2$

$= \gcd(82, 2)$ $\qquad 82 = 41 \cdot 2 + 0$

$= 2$

$$\begin{array}{r} 662 \\ -\,414 \\ \hline 248 \end{array} \qquad \begin{array}{r} 1 \\ 248 \,\big)\, 414 \\ 248 \\ \hline 166 \end{array} \qquad \begin{array}{r} 1 \\ 166 \,\big)\, 248 \\ 166 \\ \hline 82 \end{array} \qquad \begin{array}{r} 2 \\ 82 \,\big)\, 166 \\ 164 \\ \hline 2 \end{array}$$

**Proof of Euclidean Algorithm**

Let $a = qb + r$, where $a, b, q, r$ are integers
$0 \le r < |b|$.

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

Proof: $a = qb + r$ Let $d = \gcd(a,b) \Rightarrow d|a$ and $d|b$

$a - qb = r$ $d|a$ $d|b \Rightarrow d|qb$

$d|a-qb$

$\therefore d|r$

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

$\gcd(252,198) = \gcd(198,54) = \gcd(54,36) = \gcd(36,18) = 18$

$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot \underline{36} + \underline{18}$

$36 = 2 \cdot 18 + 0$

$$\begin{array}{r|l} & \ \ 1 \\ \hline 198 & 252 \\ & 198 \\ \hline & \ \ 54 \end{array} \qquad \begin{array}{r|l} & \ \ 3 \\ \hline 54 & 198 \\ & 162 \\ \hline & \ \ 36 \end{array}$$

**Theorem 6**

Let $a, b$ be positive integers. Then there exist two integers $s$ and $t$ such that

$$\gcd(a,b) = sa + tb$$

$252 = 1 \cdot 198 + 54$ $\quad$ $54 = 252 - 1 \cdot 198$

$198 = 3 \cdot 54 + 36$ $\quad$ $36 = 198 - 3 \cdot 54$

$54 = 1 \cdot \underline{36} + \underline{18}$ $\quad$ $18 = 54 - 1 \cdot 36$

$36 = 2 \cdot 18 + 0$

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \\ &= 54 - (198 - 3 \cdot 54) \\ &= 4 \cdot 54 - 1 \cdot 198 \\ &= 4(252 - 1 \cdot 198) - 198 \\ 18 &= 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$

$\gcd(252, 198) = 18$ $\quad$ $18 = s \cdot 252 + t \cdot 198$

**Lemma 3** If $p$ is prime, and $p \mid a_1 \cdot a_2 \cdots a_n$, where each $a_i$ is a positive int.,

then $p \mid a_i$ for some $i$.

**Section 4.3, Problem 15'**. Find all primes <= 30.

$\lfloor \sqrt{30} \rfloor = 5$

Use the Sieve of Eratosthenes algorithm.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~

~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~

~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

**Problem 15**. Find all positive integers that are < 30 and relatively prime to 30.

$30 = 2 \times 3 \times 5$

~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~

~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~

~~25~~ ~~26~~ ~~27~~ ~~28~~ 29