KALIKADEVI ART'S, COMMERCE & SCIENCE COLLEGE, SHIRUR(KA)

Department of Mathematics

Number Theory:

Divisibility, Prime Numbers, Greatest Common Divisor, Relative Primarily

Groups, Rings and Fields

CLASS : B.SC S.Y

MR.GHADGE R.B

Divisibility and Divisors

- We say that ***m* divides *n*** (or ***n* is divisible by *m*)** if:
  - $m > 0$

  and:
  - the ratio $\frac{n}{m}$ is an integer.
- This property underlies all number theory, so we have a notation for it:

$$m \mid n$$

and we say that *m* is a ***divisor*** of *n*

Divisibility and Divisors

- Here are some relations:
  1) If $a|1$, then $a = \pm 1$
  2) If $a|b$ and $b|a$, then $a = \pm b$
  3) Any divides 0 $b \neq 0$
  4) If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n
  5) If $a|b$ and $b|c$, then $a|c$
  6) If n is a positive number > 1, and d is the smallest divisor of n that is greater than 1, then d is prime.

Greatest Common Divisor (GCD)

- The ***greatest common divisor*** of two integers *m* and *n* is the largest integer that divides them both:

  gcd(*m*, *n*) = max{*k* | *k*|*m* and *k*|*n*}

  - Euclid's algorithm to calculate gcd(m,n), for given values $0 \le m \le n$ uses the recurrence:

$$\gcd(0, n) = n;$$

$$\gcd(m, n) = \gcd(n \bmod m, m), \qquad \text{for } m > 0$$

- So, for example, gcd(12, 18) = gcd(6,12) = gcd(0,6) = 6
  - Because any common divisor of *m* and *n* must also be a common divisor of both *m* and the number:

$$n \bmod m = n - \lfloor n/m \rfloor m$$

where $\lfloor a \rfloor$ is the *floor* function, the smallest integer less than or equal to a

Prime Numbers

- A positive integer p is called ***prime*** if it has just two divisors: 1 and p
- A positive integer that has three or more divisors is known as a ***composite***.
- Every integer > 1 is either prime or composite, but not both.
  - Note:
    - 2 is a prime
    - 1 is ***not*** a prime
- The sequence of primes starts:

  `2,3,5,7,11,13,17,19,23,29,31,37,41,...`

Greatest Common Divisor (GCD)

- The ***greatest common divisor*** of two integers *m* and *n* is the largest integer that divides them both:

  gcd(*m*, *n*) = max{*k* | *k*|*m* and *k*|*n*}

  - Euclid's algorithm to calculate gcd(m,n), for given values $0 \le m \le n$ uses the recurrence:

$$\gcd(0, n) = n;$$

$$\gcd(m, n) = \gcd(n \bmod m, m), \qquad \text{for } m > 0$$

- So, for example, gcd(12, 18) = gcd(6,12) = gcd(0,6) = 6
  - Because any common divisor of *m* and *n* must also be a common divisor of both *m* and the number:

$$n \bmod m = n - \lfloor n/m \rfloor m$$

where $\lfloor a \rfloor$ is the *floor* function, the smallest integer less than or equal to a

Generating Small Prime Numbers

- One simple way of calculating primes is to use the ***Sieve of Eratosthenes****:
    1) Write down all integers from 2 through *x*
    2) Circle 2, marking it prime, and cross out all other multiples of 2
    3) Repeatedly circle the smallest uncircled, uncrossed number and cross out all its other multiples
    4) When every number has been circled or crossed out, the circled numbers are the primes

Try a Java applet to demonstrate this algorithm.

***Eratosthenes (276 B.C. - 195 B.C.)**

Relative Primality

- Two integers *m* and *n* are ***relatively prime*** (also known as ***coprimes***) when their gcd(m,n) = 1
  - That is, they have no common factor other than 1

  For example:
    - 14 and 15 are relatively prime, despite the fact that neither one is a prime
    - 6 and 35 are relatively prime
    - 6 and 27 are not relatively prime because they are both divisible by 3.

- This is an important concept, as we shall see later...

Relative Primality

- Two integers *m* and *n* are ***relatively prime*** (also known as ***coprimes***) when their gcd(m,n) = 1
  - That is, they have no common factor other than 1

  For example:

    - 14 and 15 are relatively prime, despite the fact that neither one is a prime
    - 6 and 35 are relatively prime
    - 6 and 27 are not relatively prime because they are both divisible by 3.

- This is an important concept, as we shall see later...

Summary

- Whew!
- I realize it's a quite a bit of new stuff, and much of it is fairly abstract.
- However, I think we need some mathematical background to understand modern cryptographic algorithms.
- There's more: Modular Arithmetic, which is a very important topic for modern cryptography.