# Number Theoretic Algorithms

CS255
Chris Pollett
Mar. 22, 2006.

# Outline

- Introduction
- Elementary Number Theory Concepts

# Introduction

- Number Theory plays an important role in many cryptographic algorithms used to securely communicate over the web.
- Our goal over the next couple of weeks is to look at some of these algorithms.
- In order to do that we will need to review/ learn for the first time some number theory.
- Throughout we will be interested in large integers. This means integers which cannot be stored in one, two, or even constantly many memory locations.
- So we will be interested in the time complexity of even simple operations like +, * as a function of the number of bits in the input.
- We will assume that any operation our computer does acts on a constant number of bits at a time, say 32, 64, 128, or 256 bits.
- For example, to add two n-bit numbers takes O(n) of such operations. To multiply two n bit numbers take $O(n^2)$ operations using the grade school algorithm.

# Elementary Number Theory Concepts

- **Z** = integers = { .., -2, -1, 0, 1, 2…}
- **N** = natural numbers = {0, 1, 2, ..}
- We write d | a to mean d divides a. That is, there is some integer c, such that cd = a.
  - Notice every integer divides 0 and if a >0, if d | a then |a| >= |d|.
  - We might also say a is a **multiple** of d or d is a **divisor** of a.
  - If d |a does not hold, then we write $d \nmid a$

# More Number Concepts

- A **prime** number is a number which is divisible by only 1 and itself. 2,3, 5, 7, 11,…
- The number 1 is called a **unit** since 1*a= a*1 =a for any a.
- Other non-primes are called **composite numbers**.
- The **division theorem** says: For any integer a and any positive integer n, there are unique numbers q and 0<=r < n such that a= qn +r.
- We q = $\lfloor a/n \rfloor$ the the **quotient** and r the **remainder** or residue of the division.
- We write $[a]_n$ for {a + kn : k is in **Z**}, the equivalence class of a mod n. For example $[-3]_7$ = {..-10, -3, 4, 11 ..}.
- We $\mathbf{Z}_n$ = {$[a]_n$: 0 <= a <= a-1}. Notice this is a field where + and * come from the integers.

# Greatest Common Divisor

- If d | a and d |b then d is a **common divisor** of a and b.
- Notice if d is a common divisor of a and b, then d|(a+b) and d|(a-b) and more generally d|(ax+by)
- The largest common divisor of a and b is called the **greatest common divisor** of a and b and is denoted gcd(a,b). ex: gcd(250,150) =50
- Notice gcd(a,b) = gcd(b,a); gcd(a,b) = gcd(-a,b); gcd(a,b) = gcd(|a|, |b|); gcd(a,0) = |a|; and gcd(a,ka) = |a|.

# Some simple theorems

**Theorem** If a and b are integers, not both zero, then gcd(a,b) is the smallest positive element of the set {ax + by :x,y in **Z**}.

**Proof** Let s be the smallest positive linear combination of a and b, and let s=ax+by for some x,y. Let q = $\lfloor a/s \rfloor$. Then

a mod s = a-qs

= a - q(ax +by)

= a(1- qx) + b(-qy),

and so a mod s is a linear combination of a and b as well. But since 0 <= a mod s <= s, we have a mod s = 0, because s was supposed to be the smallest positve such linear combination. Therefore s | a and by similar reasoning s |b. So gcd(a,b) >= s. As gcd(a,b) | a and gcd(a,b) | b, by the last slide we know gcd(a,b) | s. So gcd(a,b) =s.

**Corollary** For any a and b, if d|a and d|b, then d | gcd(a,b)

**Corollary** For all integers a and b and any integer n, gcd(an, bn) =n gcd(a,b).

**Corollary** For all positive integers n, a, and b if n|ab and gcd(a,n) =1 then n | b.