CS F364
Design & Analysis of Algorithms

Problem Domain – number Theory

Modular Arithmetic:

- Groups Z_n, Z^*_n
- Size of Z^*_n
- Computing the size of Z_n^*

Congruence Arithmetic

- "congruence modulo n":
  - if a mod n = b mod n
    - then a and b are congruent modulo n
  - This is an equivalence relation.
    - Why?
- (Z_n = { 0, 1, … n-1 }, $+_n$) is a group
    - where $+_n$ refers to addition modulo n.
  - **Exercise:** *Verify the following properties*:
    - Closure
    - Associativity
    - Existence of Identity (0)
    - Existence of Inverse (a^{-1} is n-a)

Congruence Arithmetic

- $(Z^*_n = \{ x \mid 1 <= x <= n \text{ and } gcd(x,n) = 1\}, *_n)$ is a group.
  - **Exercise**:
    - *Verify Closure and Associativity*
  - Identity Element exists (a * 1 = a)
  - Existence of Inverse:
    - Is there an x such that a*x = 1 (mod n), for a in Z^*_n ?
      - i.e. Is there an x such that a*x = 1 + b*n for some +ve integer b?
    - The answer is yes, by extended Euclid's Theorem since gcd(a,n)=1
      - Furthermore, by Aryabhatia's algorithm:
        - *the inverse of any element in $(Z^*_n, *n)$ can be computed in polynomial time.*

Congruence Arithmetic

- What is the size of Z^*_n ?
  - Let $\phi(n)$ – known as Euler's phi function - denote the size of Z^*_n
- Properties of $\phi(n)$
  - $\phi(p) = p-1$ for prime p
    - Proof: for any m < p, gcd(m,p) = 1 for prime p.
  - $\phi(p^m) = p^m - p^{m-1}$
    - Proof:
      - All multiples of p (and only them) have common factors with p^m
      - Multiples of p (less than p^m) are $p, 2*p, 3*p, \ldots, (p^{m-1} - 1) * p$
      - So, $\phi(p^m) = (p^m - 1) - (p^{m-1} - 1)$ for prime p.

Congruence Arithmetic

- Properties of $\phi(n)$ [*continued*]
  - $\phi(p*q) = (p-1)(q-1)$ for primes p and q
    - Proof:
      - Only multiples of p or q or both have common factors with p*q
        - i.e. p, 2*p, ..., q*p, and q, 2*q, ...,p*q
      - And they are all distinct except for p*q
      - So $\phi(p*q) = (p*q) - p - q + 1$
  - $\phi(m*n)$ is multiplicative i.e. $\phi(m*n) = \phi(m) * \phi(n)$ if gcd(m,n) = 1
    - Proof: *Left as an exercise.*
    - **Note:** We only need to prove $\phi(p^{k1} * q^{k2}) = \phi(p^{k1}) * \phi(q^{k2})$ for primes p and q. **End of Note.**

Congruence Arithmetic

- Value of $\phi(n)$
  - If $n = p_1^{k1} * p_2^{k2} * \ldots * p_m^{km}$ for primes p_i and +ve integers ki then $\phi(n) = \Pi_i (p_i^{ki} - p_i^{ki-1})$
- Computing $\phi(n)$
  - If the prime factors of n are known then $\phi(n)$ can be computed in polynomial time
    - But computing factors is known to be "difficult".
  - Is there an alternative?
    - Consider $n = p * q$
    - Given n and $\phi(n)$, one can compute p and q in polynomial time . (How?)
      - i.e. Computing $\phi(n)$ is at least as difficult as factoring n.