ENEE 457: Computer Systems Security
09/21/16

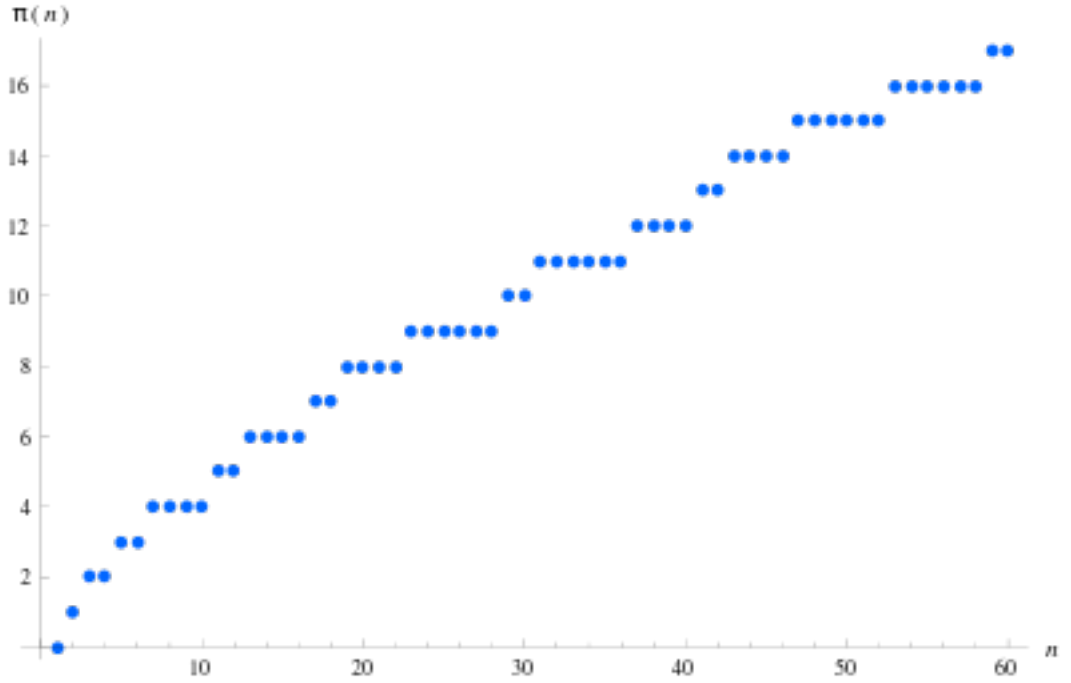
Lecture 7
Number Theory Essentials

Charalampos (Babis) Papamanthou

Department of Electrical and Computer Engineering
University of Maryland, College Park

Prime numbers

- A number x is prime if its only divisors are x and 1
- There approximately $n/\log n$ prime numbers less than n



Modulo *N* arithmetic

- We denote with x mod N the remainder of division x/N
- E.g., 18 mod 4 = 2, 16 mod 2 = 0
- If x mod N = y mod N we write $x = y$ mod N
- For example 4 = 16 mod 3
- You can add, subtract, multiply
- E.g., 6 = 18 mod 4 gives (mult. by 4) 24 = 72 mod 4
- But you cannot divide!

Beware of division modulo N

- Can you divide?
- $6 = 18 \bmod 4$
- Try to divide by 2
- $3 = 9 \bmod 4$ ➔ WRONG!!
- What happened?
- 2 DOES NOT HAVE AN INVERSE MOD 4

Greatest common divisor (gcd) of a and b

- Definition: gcd (a,b) is the greatest integer dividing both a and b
- Property: gcd(a,b) is the smallest positive integer d satisfying d = i*a+j*b for some integers a,b
- Example: gcd(8,20)=4. 4=(1)*20-2*8
- No positive number smaller than 4 can be derived by taking linear combinations of 8 and 20.

Proof

- Suppose d is the smallest positive integer d satisfying d = i*a + j*b for some i and j. Then we show that d = gcd(a,b)
- Since d = i*a + j*b, any common divisor of a and b is a divisor of d as well. But a number is always greater or equal than its divisors, so d >= gcd(a,b)
- It is a = h*d+(a mod d) so a mod d = a – hd
- But d = i*a + j*b
- So a mod d = a – hd = a – h(i*a + j*b) = (1-hi)a+(-hj)b
- But a mod d < d and d is the smallest positive integer such that d = i*a + j*b so it has to be the case that a mod d = 0 which means d divides a.
- By a similar argument we get that d divides b
- Thus d is a divisor of both a and b, so this implies d <= gcd(a,b)
- Therefore d = gcd(a,b)

Computing the gcd

- Property:
  - gcd (a,b) = gcd(b,a mod b)
- Why?
  - All common divisors of a,b are common divisors of b and a mod b: a=dx,b=dt,a mod b =d L
  - All common divisors of b,a mod b are common divisors of a and b: b = fx,a mod b=ft,a=f T
- So a and b and b and a mod b have exactly the same divisors, so gcd should also be the same
- Example
  - (412,260)→(260,152)→(152,108)→(108,44)→(44,20)→(20,4)→(4,0)

How much time do we need to compute the gcd?

- O(max(loga,logb))

Inverses mod N

- An element x has an inverse mod N iff gcd(x,N) = 1
- If x has an inverse mod N then there exists y such that
  - x * y = 1 mod N which implies x*y = k*N + 1 which gives x*y – k N = 1. Therefore 1 needs to be the gcd of x and N
  - If gcd(x,N) =1 then i*x + j*N = 1 then i*x = 1 mod N

Great Common Divisor Algorithm

```
Algorithm EuclidGCD(a, b)
    Input integers a and b
    Output gcd(a, b)

    if b = 0
        return a
    else
        return EuclidGCD(b, a mod b)
```

- Proof: We need to prove that GCD(**a**,**b**)=GCD(**b**,**a** mod **b**)
- FACTS
  - Every divisor of **a** and **b** is a divisor of **b** and (**a** mod **b**): This is because (**a** mod **b**) can be written as the sum of **a** and a multiple of **b**, i.e., **a** mod **b** = **a** + k**b**, for some integer k.
  - Similarly, every divisor of **b** and (**a** mod **b**) is a divisor of **a** and **b**: This is because **a** can be written as the sum of (**a** mod **b**) and a multiple of **b**, i.e., **a** = k**b** + (**a** mod **b**), for some integer k.
  - Therefore the set of all divisors of **a** and **b** is **the same** with the set of all divisors of **b** and (**a** mod **b**). Thus the greatest should also be the same.

Groups in Mathematics

- A group is a set, G, together with an operation • (called the group law of G) that combines any two elements a and b to form another element, denoted a • b or ab. To qualify as a group, the set and operation, (G, •), must satisfy four requirements known as the group axioms:
- **Closure**: For all a, b in G, the result of the operation, a • b, is also in G.
- **Associativity**: For all a, b and c in G, (a • b) • c = a • (b • c).
- **Identity element**: There exists an element e in G, such that for every element a in G, the equation e • a = a • e holds. Such an element is unique, and thus one speaks of the identity element.
- **Inverse element**: For each a in G, there exists an element b in G, commonly denoted a^{-1} (or −a, if the operation is denoted "+"), such that a • b = b • a = e, where e is the identity element.
- If commutivity holds, the group is called abelian

Examples of groups

- The set of integers {…-2,-1,0,1,2} is a group under addition but not under multiplication (why?).
- The set of integers modulo N {0,1,…,N-1}is a group under addition (this group is denoted Z_N)
- Is the set of reals a group under multiplication?
- The set of integers modulo N that have multiplicative inverses modulo N is a group under multiplication. We denote this group as Z*_N
  - Z*_15 = {1,2,4,7,8,11,13,14}
  - Z*_7 = {1,2,3,4,5,6} (since 7 is a prime)

Order of a group

- Order of a group is the number of elements in a group.
- Can be infinite
- ORDER(Z_N)=ORDER({0,1,…,N-1})=N
- Let (G,+) be a group of order m. Then for every element g of the group g * m = 0
- Or if (G,*) is a group of oder m. Then for every element g of the group g^m = 1
- Take all element g1,g2,…g_m. Fix arbitrary g from the group. Then we claim
  - (g1*g)*(g2*g)*...*(g_m*g) = g1*g2*…*g_m
  - This gives g^m=1
- g^x = g^{x mod m}
  - g^x=g^{k*m+(x mod m)}=(g^{m})^k*g^{x mod m} = g^{x mod m}

What is the order of Z*_N?

- Assume N = p * q where p and q are primes > 1
- Order of Z*_N is (p – 1) (q – 1)
- Denoted phi(N)
- What if N is itself a prime?
- Then order of Z*_p is p – 1

Can we define a bijection (permutation)?

- Let G be a group of order m
- If gcd(e,m)=1 then g^e is a bijection
- Suppose not. Then x^e = y^e for x \ne y which implies x = y, contradiction
- So looks like number theory gives us permutations without tables!

Cyclic groups

- Let G be a group
- The order of an element x in the group is the smallest positive integer o such that
  - x ^ o = 1
- If there exists an element g in the group that whose order is equal to the order of the group then
  - The group is called cyclic
  - All elements of the group can be generated by g as g^0,g^1,…,g^{m-1}
- Example
  - Consider Z_15. Order is 15. It is cyclic because for g = 1 we have
    - g* 15 = 1*15 = 0
    - For all other i<15 it is 1*i \ne 0 mod 15
- If the order is prime, G is cyclic and all the elements (but the identity) can serve as generators
- Z*_p is also cyclic. Example, Z*_7 is cyclic with 3 but not 2 as a generator

Computational Assumption 1: DLog

- We will be using some assumptions about problems considered to be hard
- Discrete logarithm problem
- Let G be a cyclic group of order q and let g be a generator of G
- Output an element h = g^x. Keep x secret
- Then it is very difficult (exponential in the bitlength of q) to figure out x
- **What would be a naïve algorithm for that?**

Computational Assumption 2: RSA

- Given N = pq, where p and q are primes, it is difficult to figure out p and q
- This is known as factoring assumption
- We will see an encryption scheme whose security is based on RSA
- We will see a hash function whose security is based on DLog

Chinese remainder theorem

- Let N=pq. Let
  - x mod p = a1
  - x mod q = a2
- Then
  - x **mod N** = a1* q * inverse(q in Zp)+ a2 * p * inverse(p in Zq) **mod N**
  - **Let's prove it**
  - This can be used to compute W^x mod N, for big W^x, more efficiently
  - How?
- Use of theorem
  - Say you want to compute 18^25 mod 35 (35 = 5*7)
  - Compute 18^25 mod 5 = 18^(25 mod 4) mod 5= 18^1 mod 5 = 3 = a1
  - Compute 18^25 mod 7 = 18^(25 mod 6) mod 7= 18^1 mod 7 = 4 = a2
  - Note that inverse(5 in Z_7)=3 and inverse(7 in Z_5)=3
  - Therefore the solution we are looking for is 3*7*3+4*5*3 mod 35= 18
- Used in the decryption procedure of RSA: Why cannot it be used in the encryption?