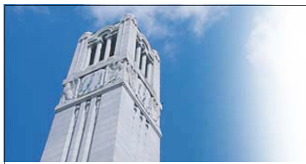

NC STATE UNIVERSITY Computer Science

CSC 474/574
Information Systems Security

Topic 2.3 Basic Number Theory

Basic Number Theory

- We are talking about integers!
- Divisor
  - We say that $b \neq 0$ <u>divides</u> a if $a = mb$ for some m, denoted $b|a$. b is a <u>divisor</u> of a.
  - If $a|1$, then $a = 1$ or -1.
  - If $a|b$ and $b|a$, then $a = b$ or $-b$.
  - Any $b \neq 0$ divides 0.
  - If $b|g$ and $b|h$, then $b|(mg+nh)$ for arbitrary integers m and n.

Basic Number Theory (Cont'd)

- Prime numbers
  - An integer $p > 1$ is a prime number if its only divisors are 1, –1 , p, and $–p$.
  - Examples: 2, 3, 5, 7, 11, 13, 17, 19, 31,…
- Any integer a > 1 can be factored in a unique way as $a = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$
  - where each $p_1 > p_2 > \dots > p_t$ are prime numbers and where each $a_i > 0$.
  - Examples: 91=13□7, 11011=13 □112 □7.

Basic Number Theory (Cont'd)

- Another view of $a|b$:
  - Let P be the set of all prime numbers
  - Represent a as $a = □_{p □ P} p^{a_p}$, where $a_p \geq 0$.
  - Represent b as $b = □_{p □ P} p^{b_p}$, where $b_p \geq 0$.
  - $a|b$ means that a_i □b_i.

Basic Number Theory (Cont'd)

- Greatest common divisor: gcd(a,b)
  - gcd(a,b) =max$\{k \mid k|a$ and $k|b\}$
  - Examples
    - gcd(6,15)=3.
    - gcd(60,24)=gcd(60,-24)=12.
    - gcd(a,0) = a.
  - gcd(a,b) can be easily derived if we can factor a and b.
- Relatively Prime Numbers
  - Integers a and b are relatively prime if gcd(a,b) = 1.
  - Example: 8 and 15 are relatively prime.

Modulo Operator

- Given any positive integer n and any integer a, we have $a = qn+r$, where $0 \le r < n$ and $q = \lfloor a/n \rfloor$
  - We write $a = r \bmod n$.
  - The remainder r is often referred to as a residue.
  - Example:
    - $2 = 12 \bmod 5$.
- Two integer a and b are said to be congruent modulo n if $a \bmod n = b \bmod n$.
  - We write $a \equiv b \bmod n$
  - Example:
    - $7 \equiv 12 \bmod 5$.

Modulo Operator (Cont'd)

- Properties of modulo operator
  - $a \equiv b \bmod n$ if $n|(a-b)$
  - $(a \bmod n) = (b \bmod n)$ implies $a \equiv b \bmod n$.
  - $a \equiv b \bmod n$ implies $b \equiv a \bmod n$.
  - $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply $a \equiv c \bmod n$.

Modular Arithmetic

- Observation:
  - The (mod n) operator maps all integers into the set of integers $\{0, 1, 2, \ldots, (n\text{-}1)\}$.
- Modular addition.
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
- Modular subtraction.
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- Modular multiplication.
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

An Exercise (n=5)

- Addition

	0	1	2	3	4
0					
1					
2					
3					
4					

- Multiplication

	0	1	2	3	4
0					
1					
2					
3					
4					

- Exponentiation
  - $92^{10} \bmod 5 =$ ____

Properties of Modular Arithmetic

- $Z_n=\{0, 1, \ldots, (n\text{-}1)\}$
- Commutative laws
  - $(w + x) \bmod n = (x + w) \bmod n$
  - $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws
  - $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
  - $[(w \times x) \times y] \bmod \mathrm{n} = [w \times (x \times y)] \bmod n$
- Distributive law
  - $[w \times (x + y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$
- Identities
  - $(0 + w) \bmod n = w \bmod n$
  - $(1 \times w) \bmod n = w \bmod n$
- Additive inverse $(-w)$
  - For each $w \in Z_n$, there exists a z such that $w + z$=0 mod n.

About Multiplicative Inverse

- Not always exist
  - Example: There doesn't exist a z such that $6 \times z = 1 \bmod 8$.

Z_8	0	1	2	3	4	5	6	7
$\times 6$	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

- An integer $a \in Z_n$ has a multiplicative inverse if $\gcd(a, n) = 1$.
- In particular, if n is a prime number, then all elements in Z_n have multiplicative inverse.

Fermat's Theorem

- If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.
  - Observation: $\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\} = \{1, 2, \ldots, (p-1)\}$.
  - $a \times 2a \times \ldots \times (p-1)a \equiv [(a \bmod p) \times (2a \bmod p) \times \ldots \times ((p-1)a \bmod p)] \bmod p$
  - $(p-1)! \times a^{p-1} \equiv (p-1)! \bmod p$
  - Thus, $a^{p-1} \equiv 1 \bmod p$.

Totient Function

- Totient function $ø(n)$: number of numbers less than n relatively prime to n
  - If n is prime, $ø(n)=n-1$
  - If $n=p\cdot q$, and p, q are primes, $ø(n)=(p-1)(q-1)$
- Examples:
  - $ø(7)$=____
  - $ø(21)$=____

Euler's Theorem

- For every a and n that are relatively prime, $a^{ø(n)} \equiv 1 \bmod n$.
  - Proof leaves as an exercise.
- Examples
  - a=3, n=10, $ø(10)$= ____ , $3^{ø(10)}$ mod 10 = ____
  - a=2, n=11, $ø(11)$=____, $2^{ø(11)}$ mod 11=____.

Modular Exponentiation

- $x^y \bmod n = x^{y \bmod ø(n)} \bmod n$
- if $y = 1 \bmod ø(n)$ then $x^y \bmod n = x \bmod n$
- Example:
  - $2^{100} \bmod 33 =$ ____

Euclid’s Algorithm

- Observation
  - $\gcd(a, b) = \gcd(b, a \bmod b)$
- Eulid (d, f), $d > f > 0$.
  1. X← d; Y← f
  2. If Y = 0 return X=gcd(d, f)
  3. R = X mod Y
  4. X ← Y
  5. Y ← R
  6. Goto 2

Extended Euclid Algorithm

- Extended Euclid (d, f)
  1. (X1, X2, X3) $\leftarrow$ (1,0,f); (Y1, Y2, Y3) $\leftarrow$ (0,1,d)
  2. If Y3=0 return X3=gcd (d, f); no inverse
  3. If Y3=1 return Y3=gcd (d, f); Y2=d^{-1} mod f
  4. Q=$\lfloor$X3/Y3$\rfloor$
  5. (T1, T2, T3) $\leftarrow$ (X1 $-$ QY1, X2 $-$ QY2, X3 $-$ QY3)
  6. (X1, X2, X3) $\leftarrow$ (Y1, Y2, Y3)
  7. (Y1, Y2, Y3) $\leftarrow$ (T1, T2, T3)
  8. Goto 2
- Observation
  – fX1 + dX2 = X3; fY1 + dY2 = Y3
  – If Y3 = 1, then fY1 + dY2 = 1
  – Y2 = d^{-1} mod f

The Power of An Integer Modulo *n*

- Consider the following expression
- $a^m \equiv 1 \bmod n$
- If *a* and *n* are relatively prime, then there is at least one integer *m* that satisfies the above equation.
  – That is, the Euler's totient function $\phi(n)$.
- The least positive exponent *m* for which the above equation holds is referred to as:
  – The order of *a* (mod *n*)
  – The exponent to which *a* belongs (mod *n*)
  – The length of the period generated by *a*.

Understanding The Order of *a* (mod *n*)

- Powers of Integers Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Observations in The Previous Table

- All sequences end in 1.
- The length of a sequence divides $\phi(19) = 18$.
  - Lengths: 1, 2, 3, 6, 9, 18.
- Some of the sequences are of length 18.
  - The base integer a generates (via powers) all nonzero integers modulo 19.

Primitive Root

- The highest possible order of a (mod n) is $\phi(n)$.
- Primitive root: If the order of a (mod n) is $\phi(n)$, then a is referred to as a primitive root of n.
  - The powers of a: $a, a^2, \ldots, a^{p-1}$ are distinct (mod n) and are all relatively prime to n.
- For a prime number p, if a is a primitive root of p, then $a, a^2, \ldots, a^{p-1}$ are all the distinct numbers mod p.

Discrete Logarithm

- Given a primitive root a for a prime number p:
  - The expression $b \equiv a^i \bmod p$, $0 \leq i \leq (p-1)$, produces the integers from 1 to $(p-1)$.
  - The exponent i is referred to as the index of b for the base a (mod p), denoted as $\mathrm{ind}_{a,p}(b)$.
  - $\mathrm{ind}_{a,p}(1)=0$, because $a^0 \bmod p = 1$.
  - $\mathrm{ind}_{a,p}(a)=1$, because $a^1 \bmod p = a$.
- Example:
  - Integer 2 is a primitive root of prime number 19

Number	1	2	3	4	5	6	7	8	9
Index	0	1	13	2	16	14	6	3	8
Number	10	11	12	13	14	15	16	17	18
Index	17	12	15	5	7	11	4	10	9

Discrete Logarithm (Cont'd)

- Consider $x=a^{\mathrm{ind}_{a,p}(x)} \bmod p$, $y=a^{\mathrm{ind}_{a,p}(y)} \bmod p$, and $xy=a^{\mathrm{ind}_{a,p}(xy)} \bmod p$,
  - $a^{\mathrm{ind}_{a,p}(xy)} \bmod p = (a^{\mathrm{ind}_{a,p}(x)} \bmod p)(a^{\mathrm{ind}_{a,p}(y)} \bmod p)$
  - $a^{\mathrm{ind}_{a,p}(xy)} \bmod p = (a^{\mathrm{ind}_{a,p}(x)+\mathrm{ind}_{a,p}(y)}) \bmod p$
  - By Euler's theorem: $a^z \equiv a^q \bmod n$ *iff* $z \equiv q \bmod \phi(p)$.
  - $\mathrm{ind}_{a,p}(xy) = \mathrm{ind}_{a,p}(x)+\mathrm{ind}_{a,p}(y) \bmod \phi(p)$.
  - $\mathrm{ind}_{a,p}(y^r) = [r \cdot \mathrm{ind}_{a,p}(y)] \bmod \phi(p)$.
- Discrete logarithm mod p: index mod p.
- Computing a discrete logarithm mod a large prime number p is in general difficult
  - Used as the basis of some public key cryptosystems.