



CSC 474

Information Systems Security

Topic 2.3 Basic Number Theory

Basic Number Theory

- We are talking about integers!
- Divisor
 - We say that $b \neq 0$ divides a if $a = mb$ for some m , denoted $b|a$. b is a divisor 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: $91 = 13 \times 7$, $11011 = 13 \times 11^2 \times 7$.

Basic Number Theory (Cont'd)

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

Basic Number Theory (Cont'd)

- Greatest common divisor: $\gcd(a,b)$
 - $\gcd(a,b) = \max \{k \mid k|a \text{ and } k|b\}$
 - 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 $0 \leq r < n$ and $q = \lfloor a/n \rfloor$.
 - We write $r = a \bmod n$.
 - 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
 - $a \equiv b \pmod n$ if $n|(a - b)$
 - $(a \pmod n) = (b \pmod n)$ implies $a \equiv b \pmod n$.
 - $a \equiv b \pmod n$ implies $b \equiv a \pmod n$.
 - $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$.

Modular Arithmetic

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

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

$$92^{10} \bmod 5 = \underline{\quad}$$

Properties of Modular Arithmetic

- $Z_n = \{0, 1, \dots, (n-1)\}$
- Commutative laws
 - $(w + x) \bmod n = (x + w) \bmod n$
 - $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws
 - $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
 - $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
- 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 $w + z = 0 \bmod n$.

About Multiplicative Inverse

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

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 $a^{p-1} \equiv 1 \pmod{p}$.
 - Observation: $\{a \pmod{p}, 2a \pmod{p}, \dots, (p-1)a \pmod{p}\} = \{1, 2, \dots, (p-1)\}$.
 - $a \times 2a \times \dots \times (p-1)a \equiv [(a \pmod{p}) \times (2a \pmod{p}) \times \dots \times ((p-1)a \pmod{p})] \pmod{p}$
 - $(p-1)! \times a^{p-1} \equiv (p-1)! \pmod{p}$
 - Thus, $a^{p-1} \equiv 1 \pmod{p}$.

Totient Function

- Totient function $\phi(n)$: number of integers less than n and relatively prime to n
 - If n is prime, $\phi(n)=n-1$
 - If $n=p*q$, and p, q are primes, $\phi(n)=(p-1)(q-1)$
- Examples:
 - $\phi(7)=$ _____
 - $\phi(21)=$ _____

Euler's Theorem

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

Modular Exponentiation

- $x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$
- if $y = 1 \bmod \phi(n)$ then $x^y \bmod n = x \bmod n$
- Example:
 - $2^{100} \bmod 33 = \underline{\hspace{2cm}}$

Euclid's Algorithm

- Observation
 - $\gcd(a, b) = \gcd(b, a \bmod b)$
- Euclid (d, f) , $d > f > 0$.
 1. $X \leftarrow d$; $Y \leftarrow f$
 2. If $Y = 0$ return $X = \gcd(d, f)$
 3. $R = X \bmod Y$
 4. $X \leftarrow Y$
 5. $Y \leftarrow R$
 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 $X3=\text{gcd}(d, f)$; no inverse
 3. If $Y3=1$ return $Y3=\text{gcd}(d, f); Y2=d^{-1} \bmod f$
 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 $fY1 + dY2 = 1$
 - $Y2 = d^{-1} \bmod f$

The Power of An Integer Modulo n

- Consider the following expression
 - $a^m \equiv 1 \pmod n$
- 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 $a \pmod n$
 - The exponent to which a belongs $\pmod n$
 - The length of the period generated by a .

Understanding The Order of $a \pmod{n}$

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

Discrete Logarithm

- Given a primitive root a for a prime number p :
 - The expression $b \equiv a^i \pmod p$, $0 \leq i \leq (p-1)$, produces the integers from 1 to $(p-1)$.
 - The exponent i is referred to as the index of b for the base $a \pmod p$, denoted as $\text{ind}_{a,p}(b)$.
 - $\text{ind}_{a,p}(1) = 0$, because $a^0 \pmod p = 1$.
 - $\text{ind}_{a,p}(a) = 1$, because $a^1 \pmod p = a$.
- 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 $x = a^{\text{ind}_{a,p}(x)} \bmod p$, $y = a^{\text{ind}_{a,p}(y)} \bmod p$, and $xy = a^{\text{ind}_{a,p}(xy)} \bmod p$,
 - $a^{\text{ind}_{a,p}(xy)} \bmod p = (a^{\text{ind}_{a,p}(x)} \bmod p)(a^{\text{ind}_{a,p}(y)} \bmod p)$
 - $a^{\text{ind}_{a,p}(xy)} \bmod p = (a^{\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)}) \bmod p$
 - By Euler's theorem: $a^z \equiv a^q \bmod p$ iff $z \equiv q \bmod \phi(p)$.
 - $\text{ind}_{a,p}(xy) = \text{ind}_{a,p}(x) + \text{ind}_{a,p}(y) \bmod \phi(p)$.
 - $\text{ind}_{a,p}(y^r) = [r \cdot \text{ind}_{a,p}(y)] \bmod \phi(p)$.
- 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.