CS 4173/5173
COMPUTER SECURITY

Basic Number Theory II

OUTLINE LAST TIME

- GCD
- Relatively prime
- (Extended) Euclid's Algorithm
- Modular Operations/Laws
- Multiplicative Inverse

PRIMES AND FACTORS

- *a* is *prime* if it has no non-trivial factors
  - examples: 2, 3, 5, 7, 11, 13, 17, 19, 31,…
- Theorem: there are infinitely many primes
- (Factorization) Any integer $a > 1$ can be factored in a unique way as $p_1^{a_1} \bullet p_2^{a_2} \bullet \ldots p_t^{a_t}$
  - where all $p_1 > p_2 > \ldots > p_t$ are prime numbers and where each $a_i > 0$

Examples:

$91 = 13^1 \times 7^1$

$11{,}011 = 13^1 \times 11^2 \times 7^1$

GREATEST COMMON DIVISOR (GCD)

- *gcd(a,b)* = max{*k* | *k*|*a* and *k*|*b*}

Example: gcd(60,24) = 12, gcd(a,0) = a

- Properties:
  - if 0 ≤ *n*, then gcd(*an*, *bn*) = *n**gcd(*a*,*b*)
  - gcd(a,0) = a
  - If gcd(*a*,*b*)=1, *a* and *b* are relatively prime.
  - For all positive integers *d*, *a*, and *b*, if *d* | *ab* and gcd(*a*,*d*) = 1
    - then *d*|*b*
  - Example:
    - 3 | 4*9, gcd(3, 4) = 1, ➔ 3 | 9

EUCLID'S ALGORITHM FOR GCD

- Insight:
  gcd(*x, y*) = gcd(*y, x* mod *y*)
- Procedure **`euclid(x, y)`** :

```
r[0] = x, r[1] = y, n = 1;
while (r[n] != 0) {
    n = n+1;
    r[n] = r[n-2] % r[n-1];
}
return r[n-1];
```

EXTENDED EUCLID'S ALGORITHM

- Let $\mathcal{LC}(x,y) = \{ux+vy : x,y \in \mathcal{Z}\}$ be the set of linear combinations of *x* and *y*
  - u and v are intergers (can be negative).
- Theorem: if *x* and *y* are any integers > 0, then gcd(*x*,*y*) is the smallest positive element of $\mathcal{LC}(x,y)$
- Euclid's algorithm can be extended to compute *u* and *v*, as well as gcd(*x*,*y*)

MODULAR ARITHMETIC

- Modular addition
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

Example: $[16 \bmod 12 + 8 \bmod 12] \bmod 12 = (16 + 8) \bmod 12 = 0$

- Modular subtraction
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

Example: $[22 \bmod 12 - 8 \bmod 12] \bmod 12 = (22 - 8) \bmod 12 = 2$

- Modular multiplication
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example: $[22 \bmod 12 \times 8 \bmod 12] \bmod 12 = (22 \times 8) \bmod 12 = 8$

MULTIPLICATIVE INVERSES

- Don't always exist!
  - Ex.: there is no *z* such that $6 \times z = 1 \bmod 8$ (m = 6 and n = 8)

z	0	1	2	3	4	5	6	7
6×z	0	6	12	18	24	30	36	42
6×z mod 8	0	6	4	2	0	6	4	2

- A positive integer $m \in \mathbb{Z}_n$ has a multiplicative inverse $m^{-1} \bmod n$ if and only if (iff) gcd(*m, n*) = 1, i.e., *m* and *n* are relatively prime

  $\Rightarrow$ If *n* is a prime number, then all positive elements in $\mathbb{Z}_n$ have multiplicative inverses

Modular Exponentiation (Power)

MODULAR POWERS

Example: show the powers of 3 mod 7

i	0	1	2	3	4	5	6	7	8
3^i	1	3	9	27	81	243	729	2187	6561
$3^i \bmod 7$	1	3	2	6	4	5	1	3	2

And the powers of 2 mod 7

i	0	1	2	3	4	5	6	7	8	9
2^i	1	2	4	8	16	32	64	128	256	512
$2^i \bmod 7$	1	2	4	1	2	4	1	2	4	1

FERMAT'S "LITTLE" THEOREM

- If p is prime
  …and a is a positive integer not divisible by p,
  …then $a^{p-1} \equiv 1 \pmod{p}$

Example: 11 is prime, 3 not divisible by 11,
so $3^{11-1} = 59049 (=5368 * 11 + 1) \equiv 1 \pmod{11}$

Example: 37 is prime, 51 not divisible by 37,
so $51^{37-1} \equiv 1 \pmod{37}$

PROOF OF FERMAT'S THEOREM

- Observation:
  - {a mod p, 2a mod p, …, (p-1)a mod p} = {1, 2, …, (p-1)}.

Example: a = 3, p = 7

a mod p = 3

2a mod p = 6

3a mod p = 2

4a mod p = 5

5a mod p = 1

6a mod p = 4

PROOF OF FERMAT'S (CONT'D)

- First,

  $[(a \bmod p) \times (2a \bmod p) \times \ldots \times ((p-1)a \bmod p)] \bmod p$

  $= [a \times 2a \times \ldots \times (p-1)a] \bmod p$ (modular multiplication)

  $= \mathbf{(p-1)! \times a^{p-1} \bmod p}$

- From observation:
  - $\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\} = \{1, 2, \ldots, (p-1)\}$.

  Then, $[(a \bmod p) \times (2a \bmod p) \times \ldots \times ((p-1)a \bmod p)] \bmod p =$

  $[1 \times 2 \times 3 \ldots \times (p-1)] \bmod p = \mathbf{(p-1)! \bmod p}$

- Thus, $a^{p-1} \equiv 1 \bmod p$.

EXAMPLE

- Compute the following
  - 3^6 mod 7
  - 13^{10} mod 11

- p is prime
- a is a positive integer not divisible by p,
- Then: $a^{p-1} \bmod p = 1$

Z_N VS Z_N^*

- Z_n is the set {0, 1, 2, …, *n*-1}, the space induced by the (mod n) operator.

- Z_n^* is the set with all positive integers less than *n* and relatively prime to *n*.
  - a subset of Z_n

- Q: Z_n^*=? when n=5.

THE TOTIENT FUNCTION

- $\phi(n) = |\mathcal{Z}_n^*|$: the number of elements in $\mathcal{Z}_n^*$.
  - $\mathcal{Z}_n^*$ is the set of integers less than *n* and relatively prime to *n*.
- Examples
  - $\phi(4)$=?
    - *GCD(1, 4) = ?*
    - *GCD(2, 4) = ?*
    - *GCD(3, 4) = ?*
  - $\phi(6)$=?
    - *GCD(1, 6) = ?*
    - *GCD(2, 6) = ?*
    - *GCD(3, 6) = ?*
    - *GCD(4, 6) = ?*
    - *GCD(5, 6) = ?*

PROPERTIES OF TOTIENT FUNCTION

a) if n is prime, then $\phi(n) = n-1$

Example: $\phi(7) = 6$

b) if $n = p^{\alpha}$, where p is prime and $\alpha > 0$, then
$\phi(n) = (p-1)*p^{\alpha-1}$

Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$

c) if $n=p*q$, and p, q are relatively prime, then
$\phi(n) = \phi(p)*\phi(q)$

Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

EXERCISE I

- $\phi(13)$=?
- $\phi(19)$=?

EXERCISE II

- $\phi(20)$=?
- $\phi(21)$=?

Tip:

if $n=p*q$, and p, q are relatively prime, then
$\phi(n) = \phi(p)*\phi(q)$

EXERCISE III

- $\phi(500)=?$

$\phi(500)$
$=\phi(125) * \phi(4)$
$= \phi(5^3) * 2$
$=(5-1) * 5^2 * 2$
$=4 * 25 * 2$
$=200$

COMPUTING TOTIENT FUNCTION

- If n is very large, It is generally hard to find the value of $\phi(n)$.
  - Finding $\phi(n)$ requires factoring n first
  - Suppose that n is some number on the order of 2^{1024}, it is computationally difficult to factor n.
  - There is no simple/efficient method!

Key: factoring a large number is computationally hard!

EULER'S THEOREM

- For every *a* and *n* that are relatively prime,
  $a^{\phi(n)} \equiv 1 \bmod n$

Example: $3^{\phi(10)} \equiv 1 \bmod 10$ (a = 3, n = 10, which are relatively prime)

Verify: $\phi(10) = \phi(2*5) = \phi(2) * \phi(5) = 1*4 = 4$

$3^{\phi(10)} = 3^4 = 81 \bmod 10 = 1$

Example: $2^{\phi(11)} \equiv 1 \bmod 11$ (a = 2, n = 11, which are relatively prime)

Verify: $\phi(11) = 11\text{-}1 = 10$

$2^{\phi(11)} = 2^{10} = 1024\ (93*11+1) \bmod 11 = 1$

MORE EULER…

- **Variant**: for all *n*, all *a* in $\mathbb{Z}_n^*$, and all non-negative *k*, $a^{k\phi(n)+1} \equiv a \bmod n$

Example: for n = 20, a = 7, $\phi(n) = 8$, and k = 3:

$$7^{3*8+1} \equiv 7 \bmod 20$$

- **Generalized Euler's Theorem**: for $n = pq$ (*p* and *q* distinct primes) and for all *a* in $\mathbb{Z}_n$, and all non-negative *k*, $a^{k\phi(n)+1} \equiv a \bmod n$

Example: for n = 15, a = 6, $\phi(n) = 8$, and k = 3:

$$6^{3*8+1} \equiv 6 \bmod 15$$

EULER'S VS FERMAT LITTLE THEOREMS

- For every a and n that are relatively prime,
  $a^{\phi(n)} \equiv 1 \bmod n$

- If n is prime,
  $a^{n-1} \equiv 1 \bmod n$

Fermat Little Theorem is a special case for Euler's Theorem!

MODULAR EXPONENTIATION

- $a^x \bmod n = a^{x \bmod \phi(n)} \bmod n$
  - *a* and *n* are relatively prime

Example: $5^7 \bmod 6 = 5^{7 \bmod \phi(6)} \bmod 6$

$= 5^{7 \bmod 2} \bmod 6 = 5$

Example: $2^{101} \bmod 33 = 2^{101 \bmod \phi(33)} \bmod 33$

$= 2^{101 \bmod 20} \bmod 33$

$= 2 \bmod 33$

$= 2$

EXERCISE

- $2^{10000} \bmod 33 = ?$
  - $= 2^{10000 \bmod \phi(33)} \bmod 33$
  - $= 2^{10000 \bmod 20} \bmod 33 = 2^0 \bmod 33 = 1$

Using: $a^x \bmod n = a^{x \bmod \phi(n)} \bmod n$

THE POWERS OF AN INTEGER, MODULO N

- Given a, consider equation: $a^m \equiv 1 \bmod n$
  - m can be 1, 2, 3, 4, …
  - Is it possible to find a value of m to satisfy the equation?
- Yes. If a and n are relatively prime, there is at least one integer m!
- Example: for $a = 3$ and $n = 7$, what is m?

m	1	2	3	4	5	6	7	8	9
$3^m \bmod 7$	3	2	6	4	5	1	3	2	6

THE POWER (CONT'D)

- The smallest positive exponent m for which the equation

$$a^m \equiv 1 \bmod n$$

holds is referred to as…

  - the *order of a (mod n),* or
  - the *length of the period generated by a*

m	1	2	3	4	5	6	7	8	9
$3^m \bmod 7$	3	2	6	4	5	1	3	2	6

UNDERSTANDING ORDER OF *A* (MOD *N*)

- If we fix *n*, and change *a* in $a^m \bmod n$ for *m = 1, 2, 3, 4, …*
- Example: *n*=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}	← order
1	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**	**18**
4	**16**	**7**	**9**	**17**	**11**	**6**	**5**	**1**	4	16	7	9	17	11	6	5	1	**9**
7	**11**	**1**	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	**3**
8	**7**	**18**	**11**	**12**	**1**	8	7	18	11	12	1	8	7	18	11	12	1	**6**
9	**5**	**7**	**6**	**16**	**11**	**4**	**17**	**1**	9	5	7	6	16	11	4	17	1	**9**
18	**1**	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	**2**

OBSERVATIONS ON THE PREVIOUS TABLE

- n = 19, then $\phi(n)$ = 18
- Some of the sequences are of length 18
  - e.g., the base a=2 generates (via powers) all members of Z_n^*
  - The base is called the primitive root (mod n)
  - The base is also called the generator when n is prime
    - a, a^2, …, a^{n-1} are all distinct numbers mod n in Z_n^*
- Key: No simple general formula to compute primitive roots modulo n
  - ➔ computational difficulty

SQUARE ROOTS

- *x* is a *non-trivial square root of 1 mod n* if it satisfies the equation $x^2 \equiv 1 \bmod n$, but *x* is neither 1 nor n-1.
  - Why n-1 is always a square root of 1 mod n?

Ex: 6 is a square root of 1 mod 35 since $6^2 \equiv 1 \bmod 35$

- Theorem: if there exists a non-trivial square root of 1 mod *n*, then *n* is not prime
  - i.e., prime numbers will not have non-trivial square roots

ROOTS (CONT'D)

- If $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where $p_1 \ldots p_k$ are distinct primes > 2, then the number of square roots (including trivial square roots) are:
  - 2^k if $\alpha_0 \leq 1$

    Example: for $n = 70 = 2^1 * 5^1 * 7^1$, $\alpha_0 = 1$, $k = 2$, and the number of square roots $= 2^2 = 4$ (1,29,41,69)
  - 2^{k+1} if $\alpha_0 = 2$

    Example: for $n = 60 = 2^2 * 3^1 * 5^1$, $k = 2$, the number of square roots $= 2^3 = 8$ (1,11,19,29,31,41,49,59)
  - 2^{k+2} if $\alpha_0 > 2$

    Example: for $n = 24 = 2^3 * 3^1$, $k = 1$, the number of square roots $= 2^3 = 8$ (1,5,7,11,13,17,19,23)

DISCRETE LOGARITHMS

- For a primitive root *a* of a number *p,* where $a^i \equiv b \bmod p$, for some $0 \leq i \leq p\text{-}1$
  - the exponent *i* is referred to as *the index of b* for the base *a* (mod *p*), denoted as $\text{ind}_{a,p}(b)$
    - sometime also denoted as $\text{dlog}_{a,p}(b)$
  - *i* is also referred to as the *discrete logarithm of b to the base a, mod p*

LOGARITHMS (CONT'D)

- Example: a=2 is a primitive root of p=19.
  it is straightforward to get $b = a^i \bmod p$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
b	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10

- How to get the discrete logarithm i from b; e.g., $\text{ind}_{2,19}(9)$

COMPUTING DISCRETE LOGARITHMS

- However, given a, b, and p, computing $i = \text{ind}_{a,p}(b)$ is generally computationally difficult

COMPUTING (CONT'D)

- Some properties of discrete logarithms
  - $\text{ind}_{a,p}(1) = 0$ because $a^0 \bmod p = 1$
  - $\text{ind}_{a,p}(a) = 1$ because $a^1 \bmod p = a$
  - $\text{ind}_{a,p}(yz) = (\text{ind}_{a,p}(y) + \text{ind}_{a,p}(z)) \bmod \phi(p)$

$\phi(p)$, *not p!*

Example: $\text{ind}_{2,19}(5*3) = (\text{ind}_{2,19}(5) + \text{ind}_{2,19}(3)) \bmod \mathbf{18 = 11}$

  - $\text{ind}_{a,p}(y^r) = (r\ \text{ind}_{a,p}(y)) \bmod \phi(p)$

Example: $\text{ind}_{2,19}(3^3) = (3*\text{ind}_{2,19}(3)) \bmod \mathbf{18 = 3}$

DIFFICULTIES IN MODULAR ARITHMETIC

- Factoring large numbers
- Computing Totient function
  - Need factoring first
- Obtaining primitive roots
- Discrete logarithm

- Public key cryptography design should leverage all these difficulties!