CS408
Cryptography & Internet Security

Lectures 11, 12, 13, 14

Basic notions of number theory

Last Time

- Randomness
- Pseudo-randomness
- PRFs, PRPs
- Security of block ciphers
  - Semantic security
  - Ciphertext indinstinguishability
  - IND-CPA security was defined in terms of a game
  - If a block cipher is a PRP, then using the cipher under the CBC or CTR modes of operation achieves semantic security

RSA Public Key Cryptosystem

Key generation:

- Select 2 large prime numbers of about the same size, p and q
- Compute $n = pq$, and $\phi(n) = (q-1)(p-1)$
- Select a random integer e, $1 < e < \phi(n)$, s.t. $\gcd(e, \phi(n)) = 1$
- Compute d, $1 < d < \phi(n)$ s.t. $ed \equiv 1 \bmod \phi(n)$

Public key: (e, n)

Private key: d

Note: p and q must remain secret

RSA Public Key Cryptosystem

Encryption

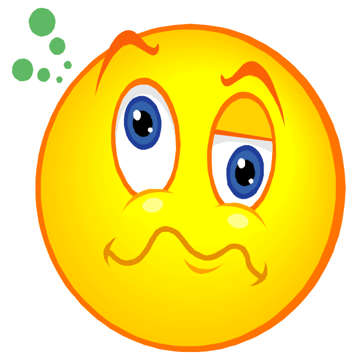
- Obtain the recipient's public key (n,e)
- Represent the message as an integer M, $0 < M < n$
- Compute $C = M^e \bmod n$
- Send ciphertext C to recipient

Decryption

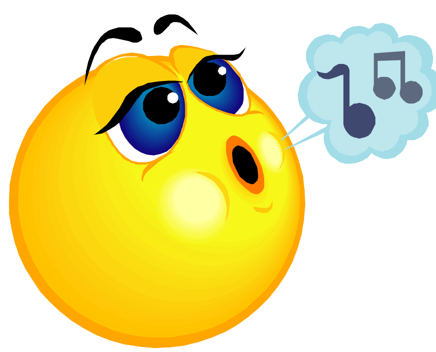
- Given a ciphertext C, use private key d to recover M: $M = C^d \bmod n$

RSA Public Key Cryptosystem

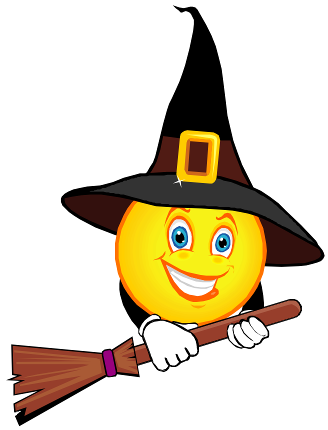
WHY IS THIS TRUE?



WHO CARES,
IT WORKS!



IT'S MAGIC!



IT'S NOT MAGIC,
IT'S MATH!

Divisibility

Definition

Given integers a and b, with $a \neq 0$, a divides b (denoted $a|b$) if ∃ integer k, s.t. $b = ak$

- a is called a **divisor** of b, and b a **multiple** of a

Propositions:

1. If $a \neq 0$, then $a|0$ and $a|a$. Also, $1|b$ for every b.
2. If $a|b$ and $b|c$, then $a|c$
3. If $a|b$ and $a|c$, then $a \mid (sb + tc)$ for all integers s and t. (We say if a divides b and c, then it divides any linear combination of b and c)

Divisibility (cont.)

Theorem

Given integers a, b such that $a>0$, $a<b$ then there exist two unique integers q and r, $0 \leq r < a$ s.t. $b = aq + r$

Prime and Composite Numbers

Definition
An integer n > 1 is called a prime number if its only positive divisors are 1 and n

Definition
Any integer number n > 1 that is not prime, is called a composite number

Example
Prime numbers: 2, 3, 5, 7, 11, 13, 17, …
Composite numbers: 4, 6, 25, 900, 17778, …

Decomposition in Product of Primes

Theorem (Fundamental Theorem of Arithmetic)
Any integer number n > 1 can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

$$n = p_1^{e_1} p_2^{e2} \dots p_k^{ek}$$

Example: 84 = 2^2 x 3 x 7

Number of Prime Numbers

Theorem

The number of prime numbers is infinite.

(for the proof, I recommend reading:

http://en.wikipedia.org/wiki/Euclid's_theorem

The proof given by Euclid is educational and quite interesting!)

Distribution of Prime Numbers

Theorem (prime number theorem)

For any real number x, the number of primes smaller than x is given by:

$$\pi(x) \approx \frac{x}{\ln x}$$

Example

We can estimate that the number of 100-digit primes is:

$\pi(10^{100}) - \pi(10^{99}) \approx 10^{100}/\ln 10^{100} - 10^{99}/\ln 10^{99} \approx 3.9 \times 10^{97}$

Greatest Common Divisor (GCD)

Definition
The greatest common divisor (gcd) of two positive integers a and b is the largest positive integer that divides both a and b

- We use the notation gcd(a,b)

Example
gcd(125, 200) = 25
gcd (5, 7) = 1

Definition
Two integers a > 0 and b > 0 are relatively prime if gcd(a, b) = 1

Example
49 and 100 are relatively prime

GCD as a Linear Combination

Theorem
Given positive integers a, b, with a > b, let d = gcd(a,b). Then there exist integers x, y such that ax + by = d

- In fact, d is the least positive integer that can be represented as ax + by
- If a and b are relatively prime, then there exist integers x, y such that ax + by = 1

Example
gcd(100, 36) = 4 **=** 4 × 100 + (-11) × 36 = 400 - 396
gcd (7, 4) = 1 = 3 x 7 + (-5) x 4 = 21 - 20

GCD and Multiplication

Theorem
Let a, b, and m be integers greater than 1.
If gcd(a, m) = gcd(b, m) = 1, then gcd(ab, m) = 1

(if a and m are relatively prime, b and m are relatively prime, then also ab and m are relatively prime)

GCD and Multiplication

Theorem
If a prime p divides a product of integers ab, then either p|a or p|b

Proof:
Assume p does not | a.
Then gcd(a,p) = 1, so there exists x and y such that ax + py = 1.
We multiply by b and get bax + bpy = b.
Since p | bax and p | pby, we have that p | (abx + bpy).
So p|b

Similarly, if we assume that p does not | b, we can show that p|a

GCD and Division

Theorem
Given integers a>0, b, q, r, such that b = aq + r, then gcd(b, a) = gcd(a, r)

Finding GCD

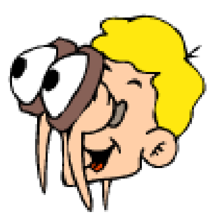
Using the Theorem: Given integers a>0, b, q, r, such that b = aq + r, then gcd(b, a) = gcd(a, r)

gcd is the last nonzero remainder:

Euclidian Algorithm

Find gcd (b, a)

while a ≠0 *do*
r ← b mod a
b ← a
a ← r
return b



Euclidian Algorithm Example

Find gcd(143, 110)

b = a x q + r

143 = 110 x 1 + 33
110 = 33 x 3 + 11
33 = 11 x 3 + 0

gcd(143, 110) = 11

Euclidian Algorithm Example

gcd(482, 1180)

1180 = 482 x 2 + 216
482 = 216 x 2 + 50
216 = 50 x 4 + 16
50 = 16 x 3 + 2
16 = 2 x 8 + 0

gcd (482, 1180) = 2

Towards Extended Euclidian Algorithm

Theorem
Given positive integers a, b, with a > b, let d = gcd(a,b).
Then there exist integers x, y such that ax + by = d

How to find such x and y?

Hint: use a modified version of the Euclidian algorithm

Iterative method

1180 = 2 x 482 + 216
482 = 2 x 216 + 50
216 = 4 x 50 + 16
50 = 3 x 16 + 2
16 = 8 x 2 + 0

gcd (482, 1180) = 2

How to write 2 as a function of 1180 and 482

$q_1 = 2$
$q_2 = 2$
$q_3 = 4$
$q_4 = 3$
$q_5 = 8$

$x_0 = 0, y_0 = 1$
$x_1 = 1, y_1 = 0$
$x_j = -q_{j-1}x_{j-1} + x_{j-2}$
$y_j = -q_{j-1}y_{j-1} + y_{j-2}$
$ax_n + by_n = gcd(a,b)$

$x_2 = -q_1 x_1 + x_0 = -2$
$x_3 = -q_2 x_2 + x_1 = -2 \times (-2) + 1 = 5$
$x_4 = -q_3 x_3 + x_2 = -4 \times 5 + (-2) = -22$
$x_5 = -q_4 x_4 + x_3 = -3 \times (-22) + 5 = 71$

Compute $y_5 = -29$

482 x 71 + 1180 x (-29) = 2 = gcd(482, 1180)

Extended Euclidian Algorithm

```
x=1;  y=0;  d=a;  r=0;  s=1;  t=b;
while (t>0) {
        q = ⌊d/t⌋
        u=x-qr;  v=y-qs;  w=d-qt
        x=r;     y=s;     d=t
        r=u;     s=v;     t=w
}
return (d, x, y)
```

Invariants:

$ax + by = d$

$ar + bs = t$

Are we there yet?

- Solving linear equations
- CRT

Modulo Operation

Definition:

Given two integers a and n:

$$a \bmod n = r \Leftrightarrow \exists q, \text{s.t. } a = q \times n + r$$
$$\underline{\text{where } 0 \le r \le n-1}$$

(so, the modulo operation finds the remainder of dividing a by n; division is done over integers)

Example:

7 mod 3 = 1, 7 = 3 x 2 + 1

-7 mod 3 = 2, -7 = -3 x 3 + 2

Congruence modulo n

Definition

Let a, b, n be integers with n≠0. Then:

$$a \equiv b \bmod n \Leftrightarrow a \bmod n = b \bmod n$$

(we read a≡b mod n as a is congruent to b mod n)

Another formulation is that a - b is a multiple of n.

n | (a-b)

Or, a = nk + b, for some k

Example

29 ≡ 14 mod 3

16 ≡ 51 mod 5

Congruence Relation

Theorem
Congruence mod n is an equivalence relation:

Reflexive: $a \equiv a \pmod{n}$
Symmetric: $a \equiv b \pmod{n}$ iff $b \equiv a \bmod n$
Transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then
$a \equiv c \pmod{n}$

Congruence Relation Properties

1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
   $a + c \equiv b + d \pmod{n}$
   $a - c \equiv b - d \pmod{n}$
   $ac \equiv bd \pmod{n}$

2. If $a \equiv b \pmod{n}$ and $d \mid n$ then:
   $a \equiv b \pmod{d}$

3. If $a \equiv b \pmod{n}$, $a \equiv b \pmod{m}$ and gcd(m, n)=1, then
   $a \equiv b \pmod{mn}$

Operations modulo n

For positive integers, a, b, n, how do we compute
a op b (mod n)? (where op is +, - , x)

1. We compute a op b as integers
2. If a op b is < n, we stop
3. If a op b ≥ n, we divide by n and take the remainder

Operations modulo n

What about division modulo n?

Proposition

Let a, b, c, n be integers with $n \neq 0$.

If $ab \equiv ac \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv c \pmod{n}$.

(In other words, if a and n are relatively prime, we can divide both sides of the congruence by a)

Example

Solve $2x + 7 \equiv 3 \pmod{17}$.

We have $2x \equiv -4 \pmod{17}$

We can divide both sides by 2, since gcd(2, 17)=1

We get $x \equiv -2 \equiv 15 \pmod{17}$

Linear Equation Modulo n

If **gcd(a, n) = 1**, then the equation

$$ax \equiv 1 \bmod n$$

has a unique solution for x, with 0< x < n.

This solution is often represented as a^{-1} mod n
(the multiplicative inverse of a).
(note that the solution is unique up to the modulo operation)

Proof: Assume there are two solutions x_1 and x_2 s.t.
$ax_1 \equiv 1 \pmod n$ and $ax_2 \equiv 1 \pmod n$
$\Rightarrow a(x_1-x_2) \equiv 0 \pmod n \Rightarrow n \mid a(x_1-x_2) \quad \Rightarrow n \mid (x_1-x_2)$
$\Rightarrow x_1-x_2=0$

How to compute x?
Using Extended Euclidian algorithm, find s and t s.t.:
as + nt = 1
Then, as = -t*n +1 = 1 (mod n), so s is the solution

Examples

Solve

$2x \equiv 1 \bmod 3$ => 2 (, 5, 8, …)
$3x \equiv 1 \bmod 7$ => 5 (, 12, 19, .
$4x \equiv 1 \bmod 5$ => 4 (, 9, 14, …)

Linear Equation Modulo n (cont.)

Let **gcd(a, n) = d**.
The equation

$$ax \equiv b \bmod n$$

has a solution **iff d | b**

Examples

Which equations have solutions?

6x ≡ 2 mod 4

6x ≡ 0 mod 3

6x ≡ 2 mod 3

6x ≡ 0 mod 2

Solving Linear Equation Modulo

To solve the equation $ax \equiv b \bmod n$

When gcd(a,n)=1, compute $x = a^{-1} b \pmod{n}$.
(obtain a^{-1} by solving $ax \equiv 1 \pmod{n}$)

When gcd(a,n) = d >1, do the following:

- If d does not divide b, there is no solution.
- If d|b, then solve the new congruence

  $$(a/d)x \equiv b/d \pmod{n/d}$$

  and get solution x_0

- The solutions of the original congruence are
  x_0, x_0+(n/d), x_0+2(n/d), …, x_0+(d-1)(n/d) (mod n).

  (so, there are d solutions)

Examples

- $2x \equiv 3 \pmod{5}$
- Since gcd(2, 5) = 1, we compute 2^{-1}, by solving $2x \equiv 1 \pmod{5}$
- 2^{-1} with respect to multiplication mod 5 is -2
  (from EEA, we have 2*(-2) + 5*1 = 1)
- We multiply both sides by -2, we get x = (-2) * 3 (mod 5), so
  x = -6 = 4 (mod 5)

- $12x \equiv 21 \pmod{39}$
- gcd(12, 39) = 3, which divides 21
- We divide by 3 to obtain the new congruence $4x \equiv 7 \pmod{13}$, which has solution $x_0 = 5$
- The solutions to the original congruence are:
  x_0, x_0 + 39/3, x_0 + 2 * 39/3
  $x \equiv$ 5, 18, 31 (mod 39)

- What about 6x = 2 mod 4?

Chinese Reminder Theorem (Sun Tzi, 3rd century AD)

Theorem

Let m, and n be integers s.t. gcd(m, n) = 1.
Given integers a and b, there exists exactly one solution x (mod mn) to the simultaneous congruences:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Example of CRT

Solve the system of equations:

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 15 \end{cases}$$

Since 80 ≡ 3 mod 7 and 80 ≡ 5 mod 15, then 80 is a solution, solution is uniquely determined modulo 7 * 15 = 105

How to do it?

1. List all numbers between 1 and 105 that are equal to 5 modulo 15, then check which ones are equal to 3 modulo 7.

   Or

2. Solve the Extended Euclidian Algorithm, get s and t s.t. 7s + 15t = 1, then compute the solution as:
   x = b*m*s + a*n*t = 5*7*s + 3*15*t

Chinese Reminder Theorem (CRT)

Theorem

Let n_1, n_2, …, n_k be integers s.t. $\gcd(n_i, n_j) = 1$ for any $i \neq j$.
Given integers a_1, a_2, …, a_k, there exists exactly one solution x (mod $n_1 n_2 \ldots n_k$) to the simultaneous congruences:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \ldots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Are we there yet?

- Fermat's Little Theorem

The Euler Phi Function: $\phi(n)$

Definition

Given an integer n, $\phi(n)$ is the number of integers in the interval [1, n] that are relatively prime to n.
(i.e., the number of integers a s.t. gcd(a, n)=1 and 0 < a <= n)

Theorem

If gcd(m,n) = 1, then $\phi(mn) = \phi(m)\,\phi(n)$

Note

We'll be using $\varphi(n)$ and $\phi(n)$ alternatively.
They both stand for the Greek letter "phi"

The Euler Phi Function

Theorem (formula for $\phi(n)$)
Let p be prime, and let e, m, n be positive integers

1) $\phi(p) = p-1$
2) $\phi(p^e) = p^e - p^{e-1}$
3) If $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$, then

$$\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$$

(in particular, if n=pq, where p, q are primes, then $\phi(n)=(p-1)(q-1)$)

Example

$\phi(7) = 6$
$\phi(2^3) = 2^3 - 2^2 = 4$
$\phi(10) = (2-1)(5-1) = 4$

Fermat's Little Theorem

Fermat's Little Theorem

If p is a prime number and a is a natural number that is not a multiple of p, then

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Example

4^{5-1} (mod 5) ≡ 256 (mod 5) ≡ 1 (mod 5)

Euler's Theorem

Euler's Theorem

Given integer n > 1, such that gcd(a, n) = 1, then

$$a^{\phi(n)} \equiv 1 \text{ (mod n)}$$

Corollary 1

Given integers n > 1 and a such that gcd(a, n) = 1, then $a^{\phi(n)-1}$ mod n is a multiplicative inverse of a mod n

Corollary 2 (principle of modular exponentiation)

Let n > 1, x, y, a be positive integers with gcd(a, n) = 1. If x ≡ y (mod ϕ(n)), then

$$a^x \equiv a^y \text{ (mod n)}$$

Consequence of Euler's Theorem

Corollary 2 (principle of modular exponentiation)
Let $n > 1$, x, y, a be positive integers with $\gcd(a, n) = 1$.
If $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof:
$x \equiv y \pmod{\phi(n)} \Rightarrow x\text{-}y$ is a multiple of $\phi(n) \Rightarrow$
$x-y = k\,\phi(n) \Rightarrow x = y + k\,\phi(n) \Rightarrow$
$a^x = a^{y+k\phi(n)} = a^y a^{k\,\phi(n)} = a^y (a^{\phi(n)})^k$
By applying Euler's theorem, we obtain
$a^x \equiv a^y \pmod{n}$

Consequence of Euler's Theorem

Corollary 2 (principle of modular exponentiation)
Let $n > 1$, x, y, a be positive integers with $\gcd(a, n) = 1$.
If $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Observations

exponent ↙

base → $x^y \pmod{n}$

- When we work with the bases, we work mod n
  (we can reduce bases mod n)
- When we work with the exponents, we work mod $\phi(n)$
  (we can reduce exponents mod $\phi(n)$)

Bases and Exponents

- When we work with the bases, we work mod n (we can reduce bases mod n)
  - When working mod n, the integers are: 0, 1, 2, …, n-2, n-1
  - n = 0 mod n; n+1 = 1 mod n; n+2 = 2 mod n; …; n+(n-2) = n-2 mod n; n+(n-1) = n-1 mod n
- When we work with the exponents, we work mod $\phi(n)$ (we can reduce exponents mod $\phi(n)$)
  - $a^0, a^1, a^2, a^3, \ldots, a^{\phi(n)-2}, a^{\phi(n)-1}$
  - $a^{\phi(n)} = a^0$ mod n; $a^{\phi(n)+1} = a^1$ mod n; $a^{\phi(n)+2} = a^2$ mod n;…; $a^{\phi(n)+(\phi(n)-1)} = a^{\phi(n)-1}$ mod n; $a^{\phi(n)+\phi(n)} = a^0$ mod n

Groups

Definition
A *group* (*G*,*) is a set *G* of elements on which a binary operation * is defined, which satisfies the following axioms:

Closure: For all $a, b \in G$, $a * b \in G$

Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$

Identity: $\exists\, e \in G$ s.t. for all $a \in G$, $a * e = a = e * a$
(*e* is called the *identity element* of the group)

Invertibility: For all $a \in G$, $\exists\, b \in G$ s. t. $a * b = b * a = e$
(*b* is called *a*'s *inverse*; sometimes we use the notation a^{-1} instead of *b*)

Groups (examples)

- (Z,+) is a group, where + is addition over integers.
- If • is multiplication over integers, is (Z,•) a group?
  No! Why not? Are all the group axioms satisfied?
  No, because not all elements in Z have multiplicative inverses.
- Let n>1 be an integer and let Z_n be the set {0, 1, 2, …, n-1}.
  Z_n is known as the set of integers modulo n.

  (Z_n,+) is a group, where + is addition modulo n.

Groups (examples)

- Let n>1 be an integer and let $Z^*_n = \{a \in Z_n \mid \gcd(a,n)=1\}$.
  (Z^*_n, •) is a group, where • is multiplication modulo n.

  (Z^*_n, •) is called the multiplicative group of Z_n.

- Let p be a prime integer and let Z^*_p be the set {1, 2, …, p-1}.

  (Z^*_p, •) is a group, where • is multiplication modulo p.

Groups (Revisit Euler's theorem)

- Let n>1 be an integer. If $a \in Z^*_n$, then $a^{\phi(n)} \equiv 1 \pmod n$

Groups (cont.)

Definition:
A group (G,*) is called an *abelian group* if the operation * is a commutative operation:
Commutative: For all $a, b \in G$, $a * b = b * a$.

Example:
(Z, +) is an abelian group

Definition
A group (G,*) is *cyclic* if $\exists\, g \in G$ s.t. any $h \in G$ can be written as $h = g^i$ for some integer i.
g is called group generator for G.

Example
Cyclic groups: $(Z^*_3, \bullet)$, $(Z^*_p, \bullet)$ where p is a prime

Order of a Group

Definition

The *order of a group* (G,*) is defined as the number of elements in the group.
We use the notation ord(G), or |G|.

Definition

A group G is *finite,* if |G| = ord(G) is finite.

Example:

The order of (Z^*_n, •) is ϕ(n). Why?
The order of (Z^*_p, •) is p-1. Why?
What is the order of (Z^*_7, •), (Z^*_{700}, •) ?

Order of a Group Element

Definition

The *order of an element a* from a group G, is the least positive integer *t* such that $a^t=e$, where *e* is the identity element of the group.

$(Z^*_n, \bullet)$: The multiplicative group of Z_n

- For the group $(Z^*_n, \bullet)$, the order of an element $a \in Z^*_n$ is the smallest positive integer *t* s.t. $a^t \equiv 1 \pmod{n}$
- If the order of $a \in Z^*_n$ is t, then $t \mid \phi(n)$
  (the order of an element divides the order of the group)

Example

Let n=21. Then Z^*_{21}={1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}.

$\phi(21) = \phi(3)\,\phi(7) = 12 = ord(Z^*_{21})$

These are the orders of elements in Z^*_{21}:

$a \in Z^*_{21}$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

$(Z^*_n, \bullet)$: The multiplicative group of Z_n

Example

- What is the order of 2 in $(Z^*_5, *)$?
  It is 4 because $2^4 \equiv 1 \bmod 5$
- What is the order of 3 in $(Z^*_{10}, *)$?
  It is 4 because $3^4 \equiv 1 \bmod 10$

Generators

Definition

Let $g \in Z^*_n$. If the order of g is $\phi(n)$, then g is said to be a generator (or a primitive element) of Z^*_n.

Example

$(Z^*_7, \bullet)$, $5^6 \equiv 1 \bmod 7$ and $\phi(7) = 6$

$5^6 = 15625$

$(Z^*_8, *)$ does not have a primitive element.

FACT

The group $(Z^*_n, \bullet)$ has primitive elements only if
n is 2, 4, p^t or $2p^t$, where p is an odd prime and $t \geq 1$.

Primitive Elements and Cyclic Groups

FACT

If Z^*_n has a generator, then Z^*_n is said to be *cyclic*.

Each primitive element (generator) can be used to generate the whole set: $Z^*_n = \{g^0, g^1, g^2, \ldots g^{\phi(n)-1}\}$

FACT

If the group $(Z^*_n, \bullet)$ is cyclic, the number of primitive elements is $\phi(\phi(n))$

OBSERVATION

$(Z^*_n, \bullet)$ is cyclic if it has primitive elements

$(Z^*_p, \bullet)$ is always cyclic (where p is a prime)

Primitive Elements

Examples

Z^*_{21} is not cyclic.
Z^*_{25} is cyclic. A generator is $g = 2$.

The Logarithm Function

Definition

The logarithm of a number *y* with respect to base *b* is the exponent to which *b* has to be raised in order to yield *y*.

In other words, the logarithm of y to base b is the number x satisfying the equation:

$$b^x = y$$

Discrete Logarithm

Definition

Let p be a prime, G = (Z^*_p, •) be a cyclic group, and g be a generator (primitive element) of G. Then, every element a of G can be written as $g^k \equiv a \bmod p$ for some integer k.

k is called the the discrete logarithm of a to base g modulo p.

Example

Z^*_{97} is cyclic group of order 96. A generator of Z^*_{97} is $g=5$.

Since $5^{32} \equiv 35 \pmod{97}$, we have that $\log_5 35 = 32$ in Z^*_{97}.

Note

Discrete logarithms can be defined for any finite cyclic group.

Modular Exponentiation

- How to efficiently compute $a^b \pmod n$?
- How to compute $2^{1234} \pmod{789}$?
- Method 1: compute $x = 2^{1234}$ and then reduce x mod 789
  - Infeasible (if a, b are 100-digit numbers, memory will overflow)
- Method 2: apply the modulo operation after each multiplication
  - Impractical: too slow, since we would need to compute 1234 modular multiplications

Modular Exponentiation (continued)

- Method 3: square and multiply
  Start with $2^2 \equiv 4 \pmod{789}$ and square both sides:

$2^4 \equiv 4^2 \equiv 16$	$2^{128} \equiv 559$
$2^8 \equiv 16^2 \equiv 256$	$2^{256} \equiv 37$
$2^{16} \equiv 256^2 \equiv 49$	$2^{512} \equiv 580$
$2^{32} \equiv 34$	$2^{1024} \equiv 286$
$2^{64} \equiv 367$	

Since 1234 = 1024 + 128 + 64 + 16 + 2, we have:
$2^{1234} \equiv 2^{1024} \cdot 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^2 = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \pmod{789}$

Note that we never needed to work with a number larger than 788^2
In general, to compute $a^b \pmod{n}$:

- at most $2 * \log_2(b)$ multiplications mod n are required
- we only need to work with numbers smaller than n^2

Using square and multiply, modular exponentiation can be achieved fast and not much memory is needed!

Announcement: programming project

- Programming project has been posted on the course website
- It is due on April 7 at 4:00pm
  - Email your program to me76@njit.edu and also CC me at crix@njit.edu
- You are allowed to work in teams of up to 2 students
- It is optional and counts for 10% of your final grade
- You can use the extra days (you have 3 extra days IN TOTAL through the entire semester to use for assignments and projects)
  - For example, you may use 1 extra day for Assignment #1, then 1 extra day for Assignment #2, and 1 extra day for the project
  - Or, you can use all 3 days for Assignment #2.
  - Or, you can use all 3 days for the Programming Project