Cryptography
CS 555

Topic 23: More Number Theory

Recap

- Polynomial time algorithms (in bit lengths $\|\boldsymbol{a}\|$, $\|\boldsymbol{b}\|$ and $\|\mathbf{N}\|$) to do important stuff
  - GCD(**a**,**b**)
  - Find inverse $\mathbf{a}^{-1}$ of **a** such that 1=[$\mathbf{a}\mathbf{a}^{-1}$ mod **N**] (if it exists)
  - PowerMod: [$\mathbf{a}^{\mathbf{b}}$ mod **N**]
  - Draw uniform sample from $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N | \gcd(N, x) = 1\}$
    - Randomized PPT algorithm

More Useful Facts

$$x, y \in \mathbb{Z}_N^* \rightarrow [xy \bmod N] \in \mathbb{Z}_N^*$$

Fact 1: Let $\boldsymbol{\phi(N)} = |\mathbb{Z}_N^*|$ then for any $x \in \mathbb{Z}_N^*$ we have

$$\left[x^{\boldsymbol{\phi(N)}} \bmod N\right] = 1$$

Example: $\mathbb{Z}_8^* = \{1,3,5,7\}$, $\phi(8) = 4$

$$\left[3^{\mathbf{4}} \bmod 8\right] = [9 \times 9 \bmod 8] = 1$$
$$\left[5^{\mathbf{4}} \bmod 8\right] = [25 \times 25 \bmod 8] = 1$$
$$\left[7^{\mathbf{4}} \bmod 8\right] = [49 \times 49 \bmod 8] = 1$$

More Useful Facts

$$x, y \in \mathbb{Z}_N^* \rightarrow [xy \bmod N] \in \mathbb{Z}_N^*$$

Fact 1: Let $\boldsymbol{\phi}(\boldsymbol{N}) = |\mathbb{Z}_N^*|$ then for any $x \in \mathbb{Z}_N^*$ we have $\left[x^{\boldsymbol{\phi}(\boldsymbol{N})} \bmod N\right] = 1$

Fact 2: Let $\boldsymbol{\phi}(\boldsymbol{N}) = |\mathbb{Z}_N^*|$ and let $N = \prod_{i=1}^{m} p_i^{e_i}$, where each p_i is a distinct prime number and $e_i > 0$ then

$$\boldsymbol{\phi}(\boldsymbol{N}) = \prod_{i=1}^{m}(p_i - 1)p_i^{e_i - 1} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$

More Useful Facts

Fact 2: Let $\boldsymbol{\phi(N)} = |\mathbb{Z}_N^*|$ and let $N = \prod_{i=1}^{m} p_i^{e_i}$, where each p_i is a distinct prime number and $e_i > 0$ then

$$\boldsymbol{\phi(N)} = \prod_{i=1}^{m}(p_i - 1)p_i^{e_i - 1} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$

Example 0: Let p be a prime so that $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$

$$\boldsymbol{\phi(p)} = p\left(1 - \frac{1}{p}\right) = p - 1$$

More Useful Facts

Fact 2: Let $\boldsymbol{\phi(N)} = |\mathbb{Z}_N^*|$ and let $N = \prod_{i=1}^{m} p_i^{e_i}$, where each p_i is a distinct prime number and $e_i > 0$ then

$$\boldsymbol{\phi(N)} = \prod_{i=1}^{m}(p_i - 1)p_i^{e_i - 1} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$

Example 1: $N = 9 = 3^2$ (m=1, e_1=2)

$$\boldsymbol{\phi(9)} = \prod_{i=1}^{1}(p_i - 1)p_i^{2-1} = 2 \times 3$$

More Useful Facts

Example 1: N = 9 = 3^2 (m=1, e_1=2)

$$\boldsymbol{\phi(9)} = \prod_{i=1}^{1}(p_i - 1)p_i^{2-1} = 2 \times 3$$

Double Check: $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$

More Useful Facts

Fact 2: Let $\boldsymbol{\phi(N)} = |\mathbb{Z}_N^*|$ and let $N = \prod_{i=1}^{m} p_i^{e_i}$, where each p_i is a distinct prime number and $e_i > 0$ then

$$\boldsymbol{\phi(N)} = \prod_{i=1}^{m}(p_i - 1)p_i^{e_i - 1} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$

Example 2: N = 15 = 5 × 3 (m=2, e_1=e_2=1)

$$\boldsymbol{\phi(15)} = \prod_{i=1}^{2}(p_i - 1)p_i^{1-1} = (5-1)(3-1) = 8$$

More Useful Facts

Example 2: N = 15 = 5×3 (m=2, e_1=e_2=1)

$$\boldsymbol{\phi(15)} = \prod_{i=1}^{2} (p_i - 1) p_i^{1-1} = (5-1)(3-1) = 8$$

Double Check: $\mathbb{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}$

I count 8 elements in $\mathbb{Z}_{15}^{*}$

More Useful Facts

Fact 2: Let $\boldsymbol{\phi(N)} = |\mathbb{Z}_N^*|$ and let $N = \prod_{i=1}^{m} p_i^{e_i}$, where each p_i is a distinct prime number and $e_i > 0$ then

$$\boldsymbol{\phi(N)} = \prod_{i=1}^{m}(p_i - 1)p_i^{e_i - 1} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$

Special Case: N = pq (p and q are distinct primes)

$$\boldsymbol{\phi(N)} = (p-1)(q-1)$$

More Useful Facts

Special Case: N = pq (p and q are distinct primes)

$$\boldsymbol{\phi(N) = (p-1)(q-1)}$$

Proof Sketch: If $x \in \mathbb{Z}_N$ is not divisible by p or q then $x \in \mathbb{Z}_N^*$**.** How many elements are not in $\mathbb{Z}_N^*$?

- **Multiples of p:** p, 2p, 3p,…,pq (q multiples of p)
- **Multiples of q:** q, 2q,…,pq (p multiples of q)
- **Double Counting?** N=pq is in both lists. Any other duplicates?
- No! cq = dp → q divides d (since, gcd(p,q)=1) and consequently $\mathrm{d} \geq q$
  - Hence, $\mathrm{dp} \geq pq = N$

More Useful Facts

Special Case: N = pq (p and q are distinct primes)

$$\boldsymbol{\phi(N) = (p-1)(q-1)}$$

Proof Sketch: If $x \in \mathbb{Z}_N$ is not divisible by p or q then $x \in \mathbb{Z}_N^*$. How many elements are not in $\mathbb{Z}_N^*$?

- **Multiples of p:** p, 2p, 3p,…,pq (q multiples of p)
- **Multiples of q:** q, 2q,…,pq (p multiples of q)
- **Answer:** p+q-1 elements are not in $\mathbb{Z}_N^*$

$$\boldsymbol{\phi(N) = N - (p + q - 1)}$$

$$\boldsymbol{= pq - p - q + 1 = (p-1)(q-1)}$$

Groups

Definition: A (finite) group is a (finite) set $\mathbb{G}$ with a binary operation $\circ$ (over G) for which we have

- (**Closure**:) For all $g, h \in \mathbb{G}$ we have $g \circ h \in \mathbb{G}$
- **(Identity**:) There is an element $e \in \mathbb{G}$ such that for all $g \in \mathbb{G}$ we have
$$g \circ e = g = e \circ g$$
- **(Inverses**:) For each element $g \in \mathbb{G}$ we can find $h \in \mathbb{G}$ such that $g \circ h = e$. We say that h is the inverse of g.
- (**Associativity:**) For all $g_1, g_2, g_3 \in \mathbb{G}$ we have
$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

We say that the group is **abelian** if

- (**Commutativity:**) For all $g, h \in \mathbb{G}$ we have $g \circ h = h \circ g$

Abelian Groups (Examples)

- **Example 1:** $\mathbb{Z}_N$ when ∘ denotes addition modulo N
- Identity: 0, since 0 ∘ x =[0+x mod N] = [x mod N].
- Inverse of x? Set x^{-1}=N-x so that [x^{-1}+x mod N] = [N-x+x mod N] = 0.

- **Example 2:** $\mathbb{Z}_N^*$ when ∘ denotes multiplication modulo N
- Identity: 1, since 1∘ x =[1(x) mod N] = [x mod N].
- Inverse of x? Run extended GCD to obtain integers a and b such that

$$ax + bN = \gcd(x, N) = 1$$

Observe that: x^{-1} = a. Why?

Abelian Groups (Examples)

- **Example 1:** $\mathbb{Z}_N$ when ∘ denotes addition modulo N
- Identity: 0, since 0 ∘ x =[0+x mod N] = [x mod N].
- Inverse of x? Set x^{-1}=N-x so that [x^{-1}+x mod N] = [N-x+x mod N] = 0.

- **Example 2:** $\mathbb{Z}_N^*$ when ∘ denotes multiplication modulo N
- Identity: 1, since 1∘ x =[1(x) mod N] = [x mod N].
- Inverse of x? Run extended GCD to obtain integers a and b such that

$$ax + bN = \gcd(x, N) = 1$$

Observe that: x^{-1} = a, since [ax mod N] = [1-bN mod N] = 1

Groups

Lemma 8.13: Let $\mathbb{G}$ be a group with a binary operation $\circ$ (over G) and let $a, b, c \in \mathbb{G}$. If $a \circ c = b \circ c$ then $a = b$.

Proof Sketch: Apply the unique inverse to c^{-1} both sides.

$a \circ c = b \circ c \rightarrow (a \circ c) \circ c^{-1} = (b \circ c) \circ c^{-1}$

$\rightarrow a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1})$

$\rightarrow a \circ (e) = b \circ (e)$

$\rightarrow a = b$

(**Remark**: it is not to difficult to show that a group has a *unique* identity and that inverses are *unique*).

Group Exponentiation

Definition: Let $\mathbb{G}$ be a group with a binary operation $\circ$ (over G) let m be a positive integer and let $g \in \mathbb{G}$ be a group element then we define

$$g^m = \underbrace{g \circ \cdots \circ g}_{\text{m times}}$$

Theorem: Let $\mathbb{G}$ be finite group with size $m = |\mathbb{G}|$ and let $g \in \mathbb{G}$ be a group element then g^m=1 (where 1 denotes the unique identity of $\mathbb{G}$).

Group Exponentiation

Theorem 8.14: Let $\mathbb{G}$ be finite group with size $\mathrm{m} = |\mathbb{G}|$ and let $\mathrm{g} \in \mathbb{G}$ be a group element then g^m=1 (where 1 denotes the unique identity of $\mathbb{G}$).

Proof: (for abelian group) Let $\mathbb{G} = \{g_1, \ldots, g_m\}$ then we claim

$$g_1 \circ \cdots \circ g_m = (g \circ g_1) \circ \cdots \circ (g \circ g_m)$$

Why? If $(g \circ g_i) = \left(g \circ g_j\right)$ then $g_j = g_i$ (by Lemma 8.13)

Group Exponentiation

Theorem 8.14: Let $\mathbb{G}$ be finite group with size $\mathrm{m} = |\mathbb{G}|$ and let $\mathrm{g} \in \mathbb{G}$ be a group element then g^m=1 (where 1 denotes the unique identity of $\mathbb{G}$).

Proof: (for abelian group) Let $\mathbb{G} = \{g_1, \ldots, g_m\}$ then we claim

$$g_1 \circ \cdots \circ g_m = (g \circ g_1) \circ \cdots \circ (g \circ g_m)$$

Because $\mathbb{G}$ is abelian we can re-arrange terms

$$g_1 \circ \cdots \circ g_m = (g_1 \circ \cdots \circ g_m)(g^m)$$

By Lemma 8.13 we have $1 = g^m$. QED

Group Exponentiation

Theorem 8.14: Let $\mathbb{G}$ be finite group with size $\mathrm{m} = |\mathbb{G}|$ and let $\mathrm{g} \in \mathbb{G}$ be a group element then g^m=1 (where 1 denotes the unique identity of $\mathbb{G}$).

Corollary 8.15: Let $\mathbb{G}$ be finite group with size $\mathrm{m} = |\mathbb{G}| > 1$ and let $\mathrm{g} \in \mathbb{G}$ be a group element then for any integer x we have $g^x = g^{[x \bmod m]}$.

Proof: $g^x = g^{qm+[x \bmod m]} = g^{[x \bmod m]}$, where q is unique integer such that x=qm+ $[x \bmod m]$

Group Exponentiation

Special Case: $\mathbb{Z}_N^*$ is a group of size $\boldsymbol{\phi(N)}$ so we have now proved

Corollary 8.22: For any $g \in \mathbb{Z}_{\mathrm{N}}^*$ and integer x we have

$$[g^x \bmod \mathrm{N}] = \left[g^{[x \bmod \boldsymbol{\phi(N)}]} \bmod \mathrm{N}\right]$$

Chinese Remainder Theorem

Theorem: Let N = pq (where gcd(p,q)=1) be given and let $f: \mathbb{Z}_{\mathrm{N}} \to \mathbb{Z}_p \times \mathbb{Z}_q$ be defined as follows

$$f(x) = ([x \; mod \; p], [x \; mod \; q])$$

then

- f is a bijective mapping (invertible)
- f and its inverse $f^{-1}: \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{\mathrm{N}}$ can be computed efficiently
- $f(x + y) = f(x) + f(y)$
- The restriction of f to $\mathbb{Z}_N^*$ yields a bijective mapping to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$
- For inputs $x, y \in \mathbb{Z}_N^*$ we have $f(x)f(y) = f(xy)$

Chinese Remainder Theorem

Application of CRT: Faster computation

Example: Compute $[11^{53} \bmod 15]$

f(11)=([-1 mod 3],[1 mod 5])

$f(11^{53}) = ([(-1)^{53} \bmod 3],[1^{53} \bmod 5]) = (-1,1)$

$f^{-1}(-1,1)=11$

Thus, $11=[11^{53} \bmod 15]$

Next Class

- Read Katz and Lindell 8.2
- Primes, Factoring and RSA