Cryptography

Lecture 18

Arkady Yerukhimovich

October 30, 2024

Outline

Lecture 17 Review

- Modern Crypto Approach
- A Little Number Theory
- Today: A Tiny Bit of Group Theory

Outline

Group Theory

Definition of a Group

A group is a set G with a binary operation $(\cdot)$ such that:

- Closure: $\forall g, h, \in G, g \cdot h \in G$
- Identity: $\exists$ element $1_G \in G$ s.t. $\forall g \in G, 1_G \cdot g = g \cdot 1_G = g$
- Inverse: $\forall g \in G, \exists h \in G$ s.t. $g \cdot h = h \cdot g = 1_G$
- Associativity: $\forall g_1, g_2, g_3 \in G, (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

Additional definitions:

- G is *abelian* if commutativity holds: $\forall g, h \in G, g \cdot h = h \cdot g$
- $|G|$ - *order* of G (number of elements in G) - For us $|G| < \infty$
- Exponentiation in G: $g^x = g \cdot g \cdots g$ (x times)

Examples:

- The integers, $\mathbb{Z}$, form an abelian group under addition
- The integers, $\mathbb{Z}$, are not a group under multiplication (no inverses)
- $\mathbb{Z}_N = \{1, \ldots, N-1\}$ is a group under addition $\mod N$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
   - Proof:

$$\begin{aligned} ac = bc \implies (ac)c^{-1} = (bc)c^{-1} &\implies a(cc^{-1}) = b(cc^{-1}) \\ &\implies a \cdot 1_G = b \cdot 1_G \implies a = b \end{aligned}$$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
   - Proof (for abelian groups):
     Consider $(gg_1), (gg_2), \ldots, (gg_m)$ where $g_1, \ldots, g_m \in G$
     Since $(gg_i) = (gg_j)$ iff $g_i = g_j$ (by [1]), each of the (gg_i) is distinct
     Now, we have that

     $$g_1 \cdot g_2 \cdots g_m = (gg_1) \cdot (gg_2) \cdots (gg_m) = g^m \cdot (g_1 \cdot g_2 \cdots g_m)$$

     First equality holds because the (gg_i) are all possible values in G.
     So, $g^m = 1$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
3. Let $|G| = m$, then for any $g \in G$ and any $x \in \mathbb{Z}$, $g^x = g^{[x \bmod m]}$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
3. Let $|G| = m$, then for any $g \in G$ and any $x \in \mathbb{Z}$, $g^x = g^{[x \bmod m]}$
   - Proof:
     Let $x = qm + r$ where $q, r \in \mathbb{Z}$ and $r = [x \bmod m]$

$$g^x = g^{qm+r} = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = 1_G^q \cdot g^r = g^r$$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
3. Let $|G| = m$, then for any $g \in G$ and any $x \in \mathbb{Z}$, $g^x = g^{[x \bmod m]}$
4. Let $|G| = m$, and let $e > 0 \in \mathbb{Z}$. Define $f_e : G \to G$ by $f_e(g) = g^e$.
   If $gcd(e, m) = 1$, then f_e is a permutation over G.
   If $d = e^{-1} \bmod m$, then $f_d = f_e^{-1}$.

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
3. Let $|G| = m$, then for any $g \in G$ and any $x \in \mathbb{Z}$, $g^x = g^{[x \bmod m]}$
4. Let $|G| = m$, and let $e > 0 \in \mathbb{Z}$. Define $f_e : G \to G$ by $f_e(g) = g^e$.
   If $gcd(e, m) = 1$, then f_e is a permutation over G.
   If $d = e^{-1} \bmod m$, then $f_d = f_e^{-1}$.
   - Proof: Enough to prove that f_d is inverse of f_e
     For any $g \in G$, we have:

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{ed} = g^{[ed \bmod m]} = g^1 = g$$

Important Properties of Groups

1. $\forall a, b, c \in G$, if $ac = bc$, then $a = b$
2. Let $|G| = m$, $\forall g \in G, g^m = 1$
3. Let $|G| = m$, then for any $g \in G$ and any $x \in \mathbb{Z}$, $g^x = g^{[x \bmod m]}$
4. Let $|G| = m$, and let $e > 0 \in \mathbb{Z}$. Define $f_e : G \to G$ by $f_e(g) = g^e$.
   If $gcd(e, m) = 1$, then f_e is a permutation over G.
   If $d = e^{-1} \bmod m$, then $f_d = f_e^{-1}$.

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
    - $g^x = g^{[x \bmod i]}$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
    - $g^x = g^{[x \bmod i]}$
    - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Examples:

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \dots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \dots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Examples:

- $\mathbb{Z}_N$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Examples:

- $\mathbb{Z}_N = < 1 >$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Examples:

- $\mathbb{Z}_N = < 1 >$
- $\mathbb{Z}_p^*$

Cyclic Groups

Notation: Let G be a group such that $|G| = m$

- For $g \in G$, define $< g >= \{g^0, g^1, \ldots\}$ – the items generated by g
- *order* of $g \in G$ is smallest $i \leq m$ such that $g^i = 1$ (Note that $i|m$)
- $< g >= \{g^0, \ldots, g^{i-1}\}$ is a *subgroup* of G
  - $g^x = g^{[x \bmod i]}$
  - $g^x = g^y$ iff $x = y \bmod i$

Cyclic Group

A group G is *cyclic* if $\exists g \in G$ s.t. order$(g) = |G|$. I.e., $< g >= G$.

- g is called the *generator* of G

Useful property: If $|G|$ is prime, then G is cyclic. Moreover, all $g \in G$ except 1 are generators

Examples:

- $\mathbb{Z}_N =< 1 >$
- $\mathbb{Z}_p^*$ – Not all $g \in \mathbb{Z}_p^*$ are generators: $< 2 >= \{1, 2, 4\} \neq \mathbb{Z}_7^*$ but, $< 3 >= \{1, 3, 9 = 2, 6, 4, 5\}$ is a generator

A Few Important Facts From Monday and Today

- mod N is an equivalence relation that respects add and multiply

A Few Important Facts From Monday and Today

- mod N is an equivalence relation that respects add and multiply
- Euclidean algorithm for finding $gcd(a, b)$

A Few Important Facts From Monday and Today

- mod N is an equivalence relation that respects add and multiply
- Euclidean algorithm for finding $gcd(a, b)$
- For G, s.t. $|G| = m$, $\forall g \in G, g^m = 1$

A Few Important Facts From Monday and Today

- mod N is an equivalence relation that respects add and multiply
- Euclidean algorithm for finding $gcd(a, b)$
- For G, s.t. $|G| = m$, $\forall g \in G, g^m = 1$
- For G, s.t. $|G| = m$, $g^x = g^{[x \bmod m]}$ for any $g \in G$ and $x \in \mathbb{Z}$

Outline

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers $\mod N$ under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers $\mod N$ under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$
- If $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$
- If $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

- Proof (for $N = pq$):
  Start with $\{1, \ldots, N-1\}$, and remove all items x s.t., $gcd(x, N) \neq 1$
  Remove $\overbrace{p, 2p, \ldots, (q-1)p}^{q-1}$ and $\overbrace{q, 2q, \ldots, (p-1)q}^{p-1}$
  $\phi(N) = (N-1) - (q-1) - (p-1) = pq - p - q + 1 = (p-1)(q-1)$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \dots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$
- If $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$
- If $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$
- If $N = \prod_i p_i^{e_i}$, $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$

The Group $\mathbb{Z}_N^*$

The group of (invertible) Integers mod N under multiplication

$$Z_N^* = \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\}$$

Question: What is the order of $\mathbb{Z}_N^*$?

Euler ϕ function

$\phi(N) = |\mathbb{Z}_N^*|$

- If N is prime, $\phi(N) = N - 1$
- If $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$
- If $N = \prod_i p_i^{e_i}$, $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$

Theorem: $\forall a \in \mathbb{Z}_N^*$, $a^{\phi(N)} = 1 \bmod N$

Group Isomorphism

Definition

Groups G and H are isomorphic ($G \simeq H$) if there exists function $f : G \to H$ such that:

- f is a bijection (i.e., one-to-one and onto)

Group Isomorphism

Definition

Groups G and H are isomorphic ($G \simeq H$) if there exists function $f : G \to H$ such that:

- f is a bijection (i.e., one-to-one and onto)
- $\forall g_1, g_2 \in G,\ f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$

in G　　　　in H

$\cdot_G$　　　　$\cdot_H$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

$\mathbb{Z}_6^*$

$f(5) = ([5 \bmod 2], [5 \bmod 3]) = (1, 2)$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1, 1)$, $2 \leftrightarrow (2, 2)$, $7 \leftrightarrow (2, 1)$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1, 1)$, $2 \leftrightarrow (2, 2)$, $7 \leftrightarrow (2, 1)$
- Compute $11^{53} \bmod 15$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1,1)$, $2 \leftrightarrow (2,2)$, $7 \leftrightarrow (2,1)$
- Compute $11^{53} \bmod 15$
    1. Apply CRT: $11 \leftrightarrow (1,2)$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1,1)$, $2 \leftrightarrow (2,2)$, $7 \leftrightarrow (2,1)$
- Compute $11^{53} \bmod 15$
    1. Apply CRT: $11 \leftrightarrow (1,2)^{53} = (1, 2^{53}) = (1,2) = 11$
    2. Use modular arithmetic mod 3: $2 = -1 \bmod 3$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1,1)$, $2 \leftrightarrow (2,2)$, $7 \leftrightarrow (2,1)$
- Compute $11^{53} \bmod 15$
  1. Apply CRT: $11 \leftrightarrow (1,2)$
  2. Use modular arithmetic $\bmod 3$: $2 = -1 \bmod 3$
  3. Simplify:

$$11^{53} = (1,2)^{53} \quad = \quad ([1^{53} \bmod 5], [(-1)^{53} \bmod 3])$$

Chinese Remainder Theorem

Theorem

Let $N = pq$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \qquad \text{and} \qquad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

With isomorphism $f(x) = ([x \bmod p], [x \bmod q])$

Using the CRT: $N = 15 = 5 \cdot 3$

- $1 \leftrightarrow (1,1)$, $2 \leftrightarrow (2,2)$, $7 \leftrightarrow (2,1)$
- Compute $11^{53} \bmod 15$
  1. Apply CRT: $11 \leftrightarrow (1,2)$
  2. Use modular arithmetic $\bmod 3$: $2 = -1 \bmod 3$
  3. Simplify:

$$\begin{aligned} 11^{53} = (1,2)^{53} &= ([1^{53} \bmod 5], [(-1)^{53} \bmod 3]) \\ &= (1, [-1 \bmod 3]) = (1,2) = 11 \end{aligned}$$

Outline

Modular Arithmetic Without a Calculator

To evaluate exponentiation $\mod N$ use the following steps:

Modular Arithmetic Without a Calculator

To evaluate exponentiation $\mod N$ use the following steps:

- If N is not prime, apply the Chinese Remainder Theorem

Modular Arithmetic Without a Calculator

To evaluate exponentiation $\mod N$ use the following steps:

- If N is not prime, apply the Chinese Remainder Theorem
- Reduce $\mod \phi(N)$ in the exponent

Modular Arithmetic Without a Calculator

To evaluate exponentiation $\mod N$ use the following steps:

- If N is not prime, apply the Chinese Remainder Theorem
- Reduce $\mod \phi(N)$ in the exponent
- Reduce $\mod N$ in the base

Modular Arithmetic Without a Calculator

To evaluate exponentiation $\mod N$ use the following steps:

- If N is not prime, apply the Chinese Remainder Theorem
- Reduce $\mod \phi(N)$ in the exponent
- Reduce $\mod N$ in the base

Useful Hints:

- Sometimes useful to use negative numbers

Modular Arithmetic Without a Calculator

$\phi(N) = 7$ $\qquad$ $a^8 = a^1 = a$

To evaluate exponentiation mod N use the following steps:

- If N is not prime, apply the Chinese Remainder Theorem
- Reduce mod $\phi(N)$ in the exponent
- Reduce mod N in the base

$a^x = a^{x \bmod \phi(N)}$

Useful Hints:

- Sometimes useful to use negative numbers
- look for things that are easy to compute (e.g., 1^{53})