Modular Arithmetic and the RSA Cryptosystem

\[ p^1 \equiv 1 \]

\[
\begin{align*}
\text{MAX}(a,b) + \text{MIN}(a,b) &= a+b \\
n|m &\text{ means that } m \text{ is a an integer multiple of } n. \\
\text{We say that “} n \text{ divides } m\text{”}. \\
\text{True: } 5|25 \ 2|-66 \ 7|35, \\
\text{False: } 4|5 \ 8|2
\end{align*}
\]

Greatest Common Divisor:

\[ \text{GCD}(x,y) = \text{greatest } k \geq 1 \text{ s.t. } k|x \text{ and } k|y. \]

Least Common Multiple:

\[ \text{LCM}(x,y) = \text{smallest } k \geq 1 \text{ s.t. } x|k \text{ and } y|k. \]

Prop:

\[ \text{GCD}(x,y) = xy/\text{LCM}(x,y) \]
\[ \text{LCM}(x,y) = xy/\text{GCD}(x,y) \]
\[ GCD(x, y) = \frac{xy}{LCM(x, y)} \]
\[ LCM(x, y) = \frac{xy}{GCD(x, y)} \]

\( x = 2^2 \times 3 = 12; \ y = 3^2 \times 5 = 45 \)

\[ GCD(12, 45) = 3 \]
\[ LCM(12, 45) = 2^2 \times 3^2 \times 5 = 180 \]
\[ x \times y = 540 \]

\[ GCD(x, y) \times LCM(x, y) = xy \]

\[ \text{MAX}(a, b) + \text{MIN}(a, b) = a + b \]

\((a \mod n)\) means the remainder when \(a\) is divided by \(n\).

If \(ad + r = n, 0 \leq r < n\)
Then \(r = (a \mod n)\)
and \(d = (a \div n)\)

(a \(\equiv\) b \[mod n\])
\(a \equiv_n b\)
“a and b are equivalent modulo n”

iff \((a \mod n) = (b \mod n)\)
iff \(n | (a - b)\)

\(31 \equiv 81 \mod 2\)

\[ 31 \equiv 81 \mod 2 \]

\[ 31 \equiv_2 81 \]

\((31 \mod 2) = 1 = (81 \mod 2)\)

\(2 | (31 - 81)\)

\(\equiv_n\) is an equivalence relation

In other words,

Reflexive:
\(a \equiv_n a\)
Symmetric:
\((a \equiv_n b) \Rightarrow (b \equiv_n a)\)
Transitive:
\((a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)\)
\( a \equiv_n b \leftrightarrow n|(a-b) \)

“\( a \) and \( b \) are equivalent modulo \( n \)”

\( \equiv_n \) induces a natural partition of the integers into \( n \) classes:

\( a \) and \( b \) are said to be in the same “residue class” or “congruence class” exactly when \( a \equiv_n b \).

Define the residue class \([i]\) to be the set of all integers that are congruent to \( i \) modulo \( n \).

Residue Classes Mod 3:

\[ [0] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]
\[ [1] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]
\[ [2] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]
\[ [-6] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]
\[ [7] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]
\[ [-1] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]

Equivalence mod \( n \) implies equivalence mod any divisor of \( n \).

If \( (x \equiv_n y) \) and \( (k|n) \)
Then: \( x \equiv_k y \)

Example: \( 10 \equiv_6 16 \Rightarrow 10 \equiv_3 16 \)

If \( (x \equiv_n y) \) and \( (k|n) \)
Then: 1) \( x+a \equiv_n y+b \)
2) \( x-a \equiv_n y-b \)
3) \( xa \equiv_n yb \)

Fundamental lemma of plus, minus, and times modulo \( n \):
Equivalently,
If \( n \mid (x-y) \) and \( n \mid (a-b) \) Then:
1) \( n \mid (x-y + a-b) \)
2) \( n \mid (x-y - [a-b]) \)
3) \( n \mid (xa-yb) \)

Proof of 3:
\[ xa-yb = a(x-y) - y(b-a) \]
\( n \mid a(x-y) \) and \( n \mid y(b-a) \)

Fundamental lemma of plus minus, and times modulo \( n \):
When doing plus, minus, and time modulo \( n \), I can at any time in the calculation replace a number with a number in the same residue class modulo \( n \)

Please calculate in your head:
\[
329 \times 666 \mod 331 \\
-2 \times 4 = -8 = 323
\]

A Unique Representation System Modulo \( n \):
We pick exactly one representative from each residue class. We do all our calculations using the representatives.

Unique representation system modulo 3
Finite set \( S = \{0, 1, 2\} \)
+ and \* defined on \( S \):

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Unique representation system modulo 3
Finite set \( S = \{0, 1, -1\} \)
+ and \* defined on \( S \):

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>
The reduced system modulo $n$:

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Define $+_n$ and $\cdot_n$:

$a +_n b = (a+b \mod n)$

$a \cdot_n b = (a*b \mod n)$

$+_n$ and $\cdot_n$ are associative binary operators from $Z_n \times Z_n \rightarrow Z_n$:

When $\diamondsuit = +_n$ or $\cdot_n$:

- **Closure** $x, y \in Z_n \implies x \diamondsuit y \in Z_n$
- **Associativity** $x, y, z \in Z_n \implies (x \diamondsuit y) \diamondsuit z = x \diamondsuit (y \diamondsuit z)$

The reduced system modulo 3

$Z_3 = \{0, 1, 2\}$

Two binary, associative operators on $Z_3$:

<table>
<thead>
<tr>
<th>$+_3$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot_3$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

The reduced system modulo 2

$Z_2 = \{0, 1\}$

Two binary, associative operators on $Z_2$:

<table>
<thead>
<tr>
<th>$+_2$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot_2$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

The Boolean interpretation of $Z_2 = \{0, 1\}$

0 means FALSE    1 means TRUE

<table>
<thead>
<tr>
<th>$+_2_{\text{XOR}}$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot_2_{\text{AND}}$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
The reduced system $Z_4 = \{0, 1, 2, 3\}$

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 2 & 3 & 0 & 1 \\
2 & 3 & 0 & 1 & 2 \\
3 & 0 & 1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

The reduced system $Z_5 = \{0, 1, 2, 3, 4\}$

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 & 0 & 1 \\
2 & 3 & 4 & 0 & 1 & 2 \\
3 & 4 & 0 & 1 & 2 & 3 \\
4 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 \\
2 & 0 & 2 & 4 & 1 & 3 \\
3 & 0 & 3 & 1 & 4 & 2 \\
4 & 0 & 4 & 3 & 2 & 1 \\
\end{array}
\]

The reduced system $Z_6 = \{0, 1, 2, 3, 4, 5\}$

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 \\
2 & 0 & 2 & 4 & 1 & 3 & 5 \\
3 & 0 & 3 & 1 & 4 & 2 & 0 \\
4 & 0 & 4 & 3 & 2 & 1 & 0 \\
5 & 0 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

An operator has the permutation property if each row and each column has a permutation of the elements.

For every $n$, $\ast_n$ on $\mathbb{Z}_n$ has the permutation property

\[
\begin{array}{c|cccc}
\ast & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 \\
2 & 0 & 2 & 4 & 1 & 3 & 5 \\
3 & 0 & 3 & 1 & 4 & 2 & 0 \\
4 & 0 & 4 & 3 & 2 & 1 & 0 \\
5 & 0 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

There are exactly 8 distinct multiples of 3 modulo 8.
There are exactly 8 distinct multiples of 3 modulo 8.
There are exactly 8 distinct multiples of 3 modulo 8.

There are exactly 2 distinct multiples of 4 modulo 8.

There is exactly 1 distinct multiple of 8 modulo 8.

There are exactly 4 distinct multiples of 6 modulo 8.
There are exactly 4 distinct multiples of 6 modulo 8

There are exactly 4 distinct multiples of 6 modulo 8

There are exactly 4 distinct multiples of 6 modulo 8

There are exactly 4 distinct multiples of 6 modulo 8

There are exactly \( \text{LCM}(n,c)/c \) distinct multiples of \( c \) modulo \( n \)

Can you see the general rule?
There are exactly $\frac{\text{LCM}(n,c)}{c}$ distinct multiples of $c$ modulo $n$.

There are exactly $\frac{n}{(nc/\text{LCM}(n,c))}$ distinct multiples of $c$ modulo $n$.

There are exactly $\frac{n}{\text{GCD}(c,n)}$ distinct multiples of $c$ modulo $n$.

The multiples of $c$ modulo $n$ is the set:

$$\{0, c, c+n, c+2n, c+3n, \ldots\}$$

$$= \{kc \mod n \mid 0 \leq k \leq \frac{n}{c}\}$$

Is there a fundamental lemma of division modulo $n$?

$$cx \equiv_n cy \Rightarrow x \equiv_n y?$$

Is there a fundamental lemma of division modulo $n$?

$$cx \equiv_n cy \Rightarrow x \equiv_n y? \text{ NO!}$$

If $c=0 \mod n$, $cx \equiv_n cy$ for any $x$ and $y$. Canceling the $c$ is like dividing by zero.

Repaired fundamental lemma of division modulo $n$?

$$c \neq 0 \mod n, \text{ } cx \equiv_n cy \Rightarrow x \equiv_n y?$$

$$2*2 \equiv_6 2*5, \text{ but not } 2 \equiv_6 5.$$  
$$6*3 \equiv_{10} 6*8, \text{ but not } 3 \equiv_{10} 8.$$
When can I divide by \( c \)?

**Theorem:** There are exactly \( n/GCD(c,n) \) distinct multiples of \( c \) modulo \( n \).

**Corollary:** If \( GCD(c,n) > 1 \), then the number of multiples of \( c \) is less than \( n \).

**Corollary:** If \( GCD(c,n) > 1 \) then you can’t always divide by \( c \).

**Proof:** There must exist distinct \( x, y < n \) such that \( c \cdot x = c \cdot y \) (but \( x \neq y \)).

---

**Fundamental lemma of division modulo \( n \).**

\( GCD(c,n)=1, \ ca \equiv_n cb \Rightarrow a \equiv_n b \)

\[
ab = ac \mod n \\
n \mid (ab-ac) \\
n \mid (ab-c) \\
n \mid b-c \quad \text{since } (a,n)=1 \\
b = c \mod n
\]

---

**Corollary for general \( c \):**

\( cx \equiv_n cy \Rightarrow x \equiv_{n/GCD(c,n)} y \)

\( cx \equiv_n cy \)

\( \Rightarrow cx \equiv_{n/(c,n)} cy \) and \( (c, n/GCD(c,n)) = 1 \)

\( \Rightarrow x \equiv_{n/(c,n)} y \)

---

\( Z_6 = \{0, 1, 2, 3, 4, 5\} \)

\( Z_6^* = \{1, 5\} \)

---

**Suppose \( GCD(x,n) =1 \) and \( GCD(y,n) =1 \)**

Let \( z = xy \) and \( z' = (xy \mod n) \)

It is obvious that \( GCD(z,n) =1 \)

It requires a moment to convince ourselves that \( GCD(z',n) =1 \)
\[Z_n^* = \{x \in \mathbb{Z}_n \mid \text{GCD}(x,n) = 1\}\]

* is an associative, binary operator. In particular, \(Z_n^*\) is closed under *:
\[x, y \in Z_n^* \implies x * y \in Z_n^*.

Proof: Let \(z = xy\). Let \(z' = z \mod n\), \(z = z' + kn\).
Suppose there exists a prime \(p > 1\) \(p|z'\) and \(p|n\).
z is the sum of two multiples of \(p\), so \(p|z\).
p|z \implies p|x \text{ or } p|y.\) Contradiction of \(x, y \in Z_n^*\)

\[
\begin{array}{c|ccccc}
\times & 1 & 5 & 7 & 11 \\
1 & 1 & 5 & 7 & 11 \\
5 & 5 & 1 & 11 & 7 \\
7 & 7 & 11 & 1 & 5 \\
11 & 11 & 7 & 5 & 1 \\
\end{array}
\]

\[\begin{array}{ccc}
1 & 2 & 4 \\
2 & 4 & 1 \\
4 & 1 & 2 \\
\end{array}\]

The column permutation property is equivalent to the right cancellation property:
\[b * a = c * a \implies b = c\]

\[
\begin{array}{ccc}
1 & 2 & \alpha & 4 \\
2 & 4 & 1 & 3 \\
4 & 3 & 1 & 2 \\
\end{array}
\]

The row permutation property is equivalent to the left cancellation property:
\[a * b = a * c \implies b = c\]

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 4 & 1 & 3 \\
3 & 3 & 1 & 4 \\
4 & 4 & 3 & 2 \\
\end{array}
\]
Euler Phi Function

\[ \Phi(n) = \text{size of } \mathbb{Z}_n^* \]

= number of 1 <= k < n that are relatively prime to n.

p prime \( \Rightarrow \mathbb{Z}_p^* = \{1,2,3,...,p-1\} \)
\( \Rightarrow \Phi(p) = p-1 \)

\[ \Phi(pq) = (p-1)(q-1) \]
if p,q distinct primes

pq = # of numbers from 1 to pq
p = # of multiples of q up to pq
q = # of multiples of p up to pq
1 = # of multiple of both p and q up to pq

\[ \Phi(pq) = pq - p - q + 1 = (p-1)(q-1) \]

The multiplicative inverse of \( a \in \mathbb{Z}_n^* \) is the unique \( b \in \mathbb{Z}_n^* \) such that \( a \cdot_n b \equiv_n 1 \). We denote this inverse by \( "a^{-1}" \) or \( "1/a" \).

The unique inverse of a must exist because the a row contains a permutation of the elements and hence contains a unique 1.

\[ *_{12} \]
\begin{array}{cccc}
1 & 5 & 7 & 11 \\
5 & 1 & 7 & 11 \\
7 & 11 & 1 & 5 \\
11 & 1 & 7 & 5 \\
\end{array}

\[ \mathbb{Z}_{12}^* = \{1,5,7,11\} \]
\( \phi(12) = 4 \)

Let's consider how we do arithmetic in \( \mathbb{Z}_n \) and in \( \mathbb{Z}_n^* \)

The additive inverse of \( a \in \mathbb{Z}_n \) is the unique \( b \in \mathbb{Z}_n \) such that \( a +_n b \equiv_n 0 \).
We denote this inverse by \( "-a" \).

It is trivial to calculate:

\( "-a" = (n-a) \).
\[ Z_n = \{0, 1, 2, \ldots, n-1\} \]

\[ Z_n^* = \{ x \in Z_n \mid \gcd(x, n) = 1 \} \]

Define \( +n \) and \( *n \):

\[ a +n b = (a+b \mod n) \]
\[ a *n b = (a*b \mod n) \]

\[ c *n (a +n b) \equiv (c *n a) +n (c *n b) \]

\(<Z_n, +n>\):
1. Closed
2. Associative
3. 0 is identity
4. Additive Inverses
5. Cancellation
6. Commutative

\(<Z_n, *n>\):
1. Closed
2. Associative
3. 1 is identity
4. Multiplicative Inverses
5. Cancellation
6. Commutative

The multiplicative inverse of \( a \in Z_n^* \) is the unique \( b \in Z_n^* \)
such that \( a *n b \equiv_n 1 \). We denote this inverse by \( "a^{-1}" \) or \( "1/a" \).

Efficient algorithm to compute \( a^{-1} \) from \( a \) and \( n \).

Execute the Extended Euclid Algorithm on \( a \) and \( n \) (previous lecture). It will give two integers \( r \) and \( s \) such that:
\[ ra + sn = (a,n) = 1 \]
Taking both sides \( \mod n \), we obtain:
\[ rn \equiv_1 1 \]
Output \( r \), which is the inverse of \( a \).

Fundamental lemma of powers?

If \( (a \equiv_n b) \) Then \( x^a \equiv_n x^b \)?

No!
\[(16 \equiv_{15} 1), \text{ but it is not the case that: } 2^1 \equiv_{15} 2^{16} \]

Calculate \( a^b \mod n \):
Except for \( b \), work in a reduced mod system to keep all intermediate results less than \( \log_2(n) + 1 \) bits long.

Phase I (Repeated Multiplication)
For \( \lfloor \log b \rfloor \) steps
- multiply largest so far by \( a \)
- \( a, a^2, a^3, \ldots \)

Phase II (Make \( a^b \) from bits and pieces)
- Expand \( n \) in binary to see how \( n \) is the sum powers of 2.
- Assemble \( a^b \) by multiplying together appropriate powers of \( a \).

Two names for the same set:

\[ Z_n^* = Z_n^a \]
\[ Z_n^a = \{ a *n x \mid x \in Z_n^* \}, a \in Z_n^* \]
Two products on the same set:

\[ Z_n^a = \{ a \star_n x \mid x \in Z_n^\ast \}, a \in Z_n^\ast \]

\[ \prod x \equiv_n \prod ax \quad [\text{as } x \text{ ranges over } Z_n^\ast] \]

\[ \prod x \equiv_n \prod (a^{\text{size of } Z_n^\ast}) \quad [\text{Commutativity}] \]

\[ 1 = a^{\text{size of } Z_n^\ast} \quad [\text{Cancellation}] \]

\[ a^{\phi(n)} = 1 \]

---

Euler’s Theorem

\[ a \in Z_n^\ast, a^{\phi(n)} \equiv_n 1 \]

---

Fermat’s Little Theorem

\[ p \text{ prime, } a \in Z_p^\ast \Rightarrow a^{p-1} \equiv_p 1 \]

---

Fundamental lemma of powers.

Suppose \( x \in Z_n^\ast \), and \( a, b, n \) are naturals.

If \( a \equiv_n b \) Then \( x^a \equiv_n x^b \)

Equivalently,

\[ x^a \equiv_n x^b \mod \phi(n) \]

---

Defining negative powers.

Suppose \( x \in Z_n^\ast \), and \( a, n \) are naturals.

\( x^{-a} \) is defined to be the multiplicative inverse of \( x^a \)

\[ x^{-a} = (x^a)^{-1} \]

---

Rule of integer exponents

Suppose \( x, y \in Z_n^\ast \), and \( a, b \) are integers.

\( (xy)^{-1} \equiv_n x^{-1} y^{-1} \)

\[ x^a x^b \equiv_n x^{a+b} \]

---

Lemma of integer powers.

Suppose \( x \in Z_n^\ast \), and \( a, b \) are integers.

If \( a \equiv_n b \) Then \( x^a \equiv_n x^b \)

Equivalently,

\[ x^a \equiv_n x^b \mod \phi(n) \]
Quick raising to power.

\[
\begin{align*}
\langle Z_n, + \rangle & \quad \langle Z_n^*, * \rangle \\
1. & \text{Closed} & 1. & \text{Closed} \\
2. & \text{Associative} & 2. & \text{Associative} \\
3. & \text{0 is identity} & 3. & \text{1 is identity} \\
4. & \text{Additive Inverses} & 4. & \text{Multiplicative Inverses} \\
& \text{Fast + and -} & & \text{Fast * and /} \\
5. & \text{Cancellation} & 5. & \text{Cancellation} \\
6. & \text{Commutative} & 6. & \text{Commutative}
\end{align*}
\]

Euler Phi Function

\[
\Phi(n) = \text{size of } Z_n^*
\]

\[p \text{ prime } \Rightarrow Z_p^* = \{1, 2, 3, \ldots, p-1\} \]

\[
\Phi(p) = p-1
\]

\[
\phi(pq) = (p-1)(q-1)
\]

if \(p,q\) distinct primes

---

The RSA Cryptosystem

Rivest, Shamir, and Adelman (1978)

RSA is one of the most used cryptographic protocols on the net. Your browser uses it to establish a secure session with a site.

---

Pick secret, random \(k\)-bit primes: \(p,q\)

"Publish": \(n = pq\)

\[
\Phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)
\]

Pick random \(e \in Z_{\Phi(n)}^*\)

"Publish": \(e\)

Compute \(d = \text{inverse of } e \text{ in } Z_{\Phi(n)}^*\)

Hence, \(e \cdot d = 1 \mod \Phi(n)\)

"Private Key": \(d\)

---

\(p,q\) random primes, \(e\) random \(\in Z_{\Phi(n)}^*\)

\(n = pq\)

\(e \cdot d = 1 \mod \Phi(n)\)

\(\text{n,e is my public key. Use it to send a message to me.}\)

---

\(p,q\) prime, \(e\) random \(\in Z_{\Phi(n)}^*\)

\(n = pq\)

\(e \cdot d = 1 \mod \Phi(n)\)

\(\text{n,e}\)

\(m\)
\(n, e\)

\[p, q \text{ prime, } e \text{ random } \in \mathbb{Z}^*\]

\[n = pq\]

\[e \cdot d = 1 \mod \phi(n)\]

\[m^e \mod n\]