Great Theoretical Ideas in Computer Science

The reduced system modulo $n$:
$$Z_n = \{0, 1, 2, \ldots, n-1\}$$

Define operations $+_n$ and $*_n$:
$$a +_n b = (a+b \mod n)$$
$$a *_n b = (a*b \mod n)$$

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

For every $n$, $+_n$ on $Z_n$ has the permutation property

An operator has the permutation property if each row and each column has a permutation of the elements.
What about multiplication?
Does \( *_6 \) on \( \mathbb{Z}_6 \) have the permutation property?

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<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>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

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

No!

Fundamental lemma of plus, minus, and times modulo \( n \):
If \( (x \equiv_n y) \) and \( (a \equiv_n b) \). Then
1) \( x + a \equiv_n y + b \)
2) \( x - a \equiv_n y - b \)
3) \( x \cdot a \equiv_n y \cdot b \)

Is there a fundamental lemma of division modulo \( n \)?

\[ cx \equiv_n cy \Rightarrow x \equiv_n y \ ? \]

No!

When can’t I divide by \( c \)?

If \( \text{GCD}(c,n) > 1 \) then you can’t always divide by \( c \).

Fundamental lemma of division modulo \( n \).
If \( \text{GCD}(c,n)=1 \), then \( ca \equiv_n cb \Rightarrow a \equiv_n b \)

So
Consider the set
\[ \mathbb{Z}_n^* = \{ x \in \mathbb{Z}_n \mid \text{GCD}(x,n) = 1 \} \]

Multiplication over this set \( \mathbb{Z}_n^* \) will have the cancellation property.

Euler Phi Function \( \phi(n) \)
Define \( \phi(n) \)
\[ \phi(n) = \text{size of } \mathbb{Z}_n^* \]
\[ = \text{number of } 1 \leq k < n \text{ that are relatively prime to } n. \]
For *n on \( \mathbb{Z}_n \) the following properties hold:

[Closure] \( x, y \in \mathbb{Z}_n \Rightarrow x *_n y \in \mathbb{Z}_n \)

[Associativity] \( x, y, z \in \mathbb{Z}_n \Rightarrow (x *_n y) *_n z = x *_n (y *_n z) \)

[Commutativity] \( x, y \in \mathbb{Z}_n \Rightarrow x *_n y = y *_n x \)

What are the properties of \( \mathbb{Z}_n \)?

For \( \mathbb{Z}_n \) the following properties hold:

[Closure] \( x, y \in \mathbb{Z}_\phi(n) \Rightarrow x *_{\phi(n)} y \in \mathbb{Z}_\phi(n) \)

[Associativity] \( x, y, z \in \mathbb{Z}_\phi(n) \Rightarrow (x *_{\phi(n)} y) *_{\phi(n)} z = x *_{\phi(n)} (y *_{\phi(n)} z) \)

[Commutativity] \( x, y \in \mathbb{Z}_\phi(n) \Rightarrow x *_{\phi(n)} y = y *_{\phi(n)} x \)
Efficient algorithm to find multiplicative inverse $a^{-1}$ from $a$ and $n$.

Extended Euclidean Algorithm ($a, n$)

Get $r, s$ such that $ra + sn = \gcd(a, n) = 1$

So $ra \equiv 1 \pmod{n}$

Output: $r$ is the multiplicative inverse of $a$ in $\mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$

Define $\ast_n$ and $\ast_n^*$:

$a \ast_n b = (a + b) \mod n$
$a \ast_n^* b = (a \cdot b) \mod n$

$\langle \mathbb{Z}_n, \ast_n \rangle$

1. Closed
2. Associative
3. $0$ is identity
4. Additive Inverses
5. Cancellation
6. Commutative

$\langle \mathbb{Z}_n^*, \ast_n^* \rangle$

1. Closed
2. Associative
3. $1$ is identity
4. Multiplicative Inverses
5. Cancellation
6. Commutative

$\Gamma(a \ast_n b) \equiv (\Gamma(a) \ast_n \Gamma(b)) \pmod{n}$

Fundamental Lemmas until now

For $x, y, a, b$ in $\mathbb{Z}_n^*$, $(x \equiv_n y)$ and $(a \equiv_n b)$.
Then

1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x \ast_n a \equiv_n y \ast_n b$

For $a, b, c$ in $\mathbb{Z}_n^*$
then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Fundamental Lemma of powers?

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

NO!

$(2 \equiv_3 5)$, but it is not the case that:

$2^2 \equiv_3 2^5$

By the permutation property, two names for the same set:

$\mathbb{Z}_n^* = a\mathbb{Z}_n^*$

where

$a\mathbb{Z}_n^* = \{a \ast_n x \mid x \in \mathbb{Z}_n^*\}, \quad a \in \mathbb{Z}_n^*$

Example:

\begin{tabular}{|c|c|c|c|c|}
\hline
$a$ & 1 & 2 & 3 & 4 \\
\hline
$1$ & 1 & 2 & 3 & 4 \\
\hline
$2$ & 2 & 4 & 1 & 3 \\
\hline
$3$ & 3 & 1 & 4 & 2 \\
\hline
$4$ & 4 & 3 & 2 & 1 \\
\hline
\end{tabular}
Two products on the same set:

\[ Z_n^* = aZ_n^* \]

\[ aZ_n^* = \{ a \cdot x \mid x \in Z_n^* \}, a \in Z_n^* \]

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

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

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

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

---

**Euler’s Theorem**

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

**Fermat’s Little Theorem**

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

---

**Correct** Fundamental lemma of powers.

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

If \( a \equiv_{\phi(n)} b \) Then \( x^a \equiv_n x^b \)

Equivalently,

\( x^a \equiv_n x^a \mod \phi(n) \)

---

**Defining negative powers**

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

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

\( x^a y^b \equiv_n x^{a+b} \)

---

**A note about exponentiation**
How do you calculate

\[ 26666666666666 \mod 7 \]

**Fundamental lemma of powers.**
Suppose \( x \in Z_n^* \) and \( a, n \) are naturals.
\[ x^a \equiv x^{a \mod \Phi(n)} \mod n \]

**Time to compute**
To compute \( a^x \mod n \) for \( a \in Z_n^* \)
first, get \( x' = x \mod \Phi(n) \)
By Euler’s theorem: \( a^x = a^{x'} \mod n \)
Hence, we can calculate \( a^{x'} \) where \( x' \cdot n \).
But still that might take \( x' \approx n \) steps
if we calculate \( a, a^2, a^3, a^4, \ldots, a^x \).

**Faster exponentiation**
How do you compute \( a^{x'} \) fast?
Suppose \( x' = 2^k \)
Suppose \( 2^k \leq x' < 2^{k+1} \)

\[
\begin{align*}
    a &\rightarrow a^2 \mod n \\
    &\rightarrow a^4 \mod n \\
    &\vdots \\
    &\rightarrow a^{2^{k-1}} \mod n \\
    &\rightarrow a^{2^k} \mod n
\end{align*}
\]

\[ \text{multiply together the appropriate powers} \]

**How much time did this take?**
Only \( 2 \log x' \) multiplications

Instead of \( (x'-1) \) multiplications

Ok, back to number theory
Agreeing on a secret

Alice and Bob have never talked before but they want to agree on a secret...

How can they do this?

Diffie-Hellman Key Exchange

Alice:
- Picks prime $p$, and a value $g$ in $\mathbb{Z}_p^*$
- Picks random $a$ in $\mathbb{Z}_p^*$
- Sends over $p$, $g$, $g^a \pmod{p}$

Bob:
- Picks random $b$ in $\mathbb{Z}_p^*$, and sends over $g^b \pmod{p}$

Now both can compute $g^{ab} \pmod{p}$

What about Eve?

Alice:
- Picks prime $p$, and a value $g$ in $\mathbb{Z}_p^*$
- Picks random $a$ in $\mathbb{Z}_p^*$
- Sends over $p$, $g$, $g^a \pmod{p}$

Bob:
- Picks random $b$ in $\mathbb{Z}_p^*$, and sends over $g^b \pmod{p}$

Now both can compute $g^{ab} \pmod{p}$

If Eve’s just listening in, she sees $p$, $g$, $g^a$, $g^b$

It’s believed that computing $g^{ab} \pmod{p}$ from just this information is not easy...

btw, discrete logarithms seem hard

Discrete-Log:
- Given $p$, $g$, $g^a \pmod{p}$, compute $a$

How fast can you do this?

If you can do discrete-logs fast, you can solve the Diffie-Hellman problem fast.

How about the other way? If you can break the DH key exchange protocol, do discrete logs fast?

The RSA Cryptosystem

Our dramatis personae

Rivest
Shamir
Adleman
Euler
Fermat
Pick secret, random large primes: \( p, q \)
Multiply \( n = p \cdot q \)
“Publish”: \( n \)

\[
\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)
\]
Pick random \( e \in \mathbb{Z}_{\phi(n)}^{*} \)
“Publish”: \( e \)

Compute \( d = \text{inverse of } e \text{ in } \mathbb{Z}_{\phi(n)}^{*} \)
Hence, \( e \cdot d = 1 \mod \phi(n) \)
“Private Key”: \( d \)

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

How hard is cracking RSA?

If we can factor products of two large primes, can we crack RSA?

If we know \( \phi(n) \), can we crack RSA?

How about the other way? Does cracking RSA mean we must do one of these two?
We don’t know...

Fundamental lemma of powers
Euler phi function \( \phi(n) = |\mathbb{Z}_n| \)
Euler’s theorem
Fermat’s little theorem
Fast exponentiation
Diffie-Hellman Key Exchange
RSA algorithm