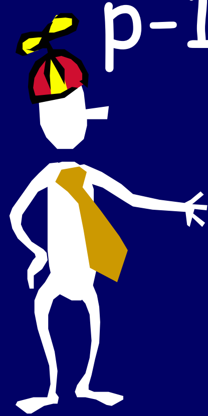
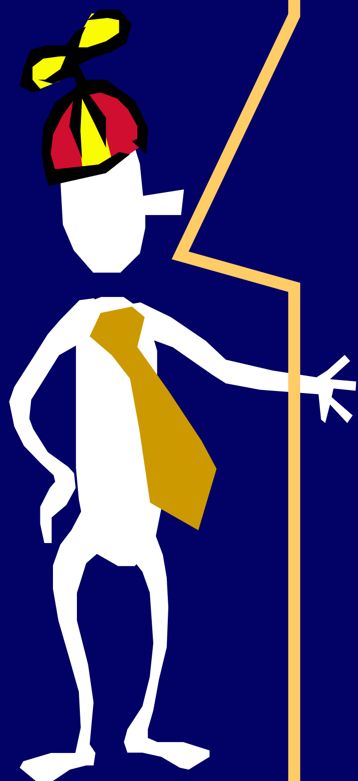
Great Theoretical Ideas In Computer Science

Steven Rudich CS 15-251 Spring 2004

Lecture 8 Feb 5, 2004 Carnegie Mellon University

Modular Arithmetic and the RSA Cryptosystem

 $^{p-1} \equiv_p 1$



n|m means that m is a an integer multiple of n.

We say that “n divides m”.

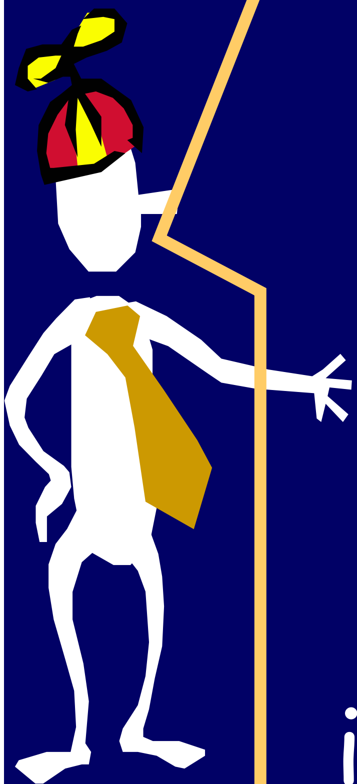
True: 5|25 2|-66 7|35,
False: 4|5 8|2

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

If $ad + r = n$, $0 \leq r < n$

Then $r = (a \bmod n)$

and $d = (a \text{ div } n)$



Modular equivalence of integers a and b:

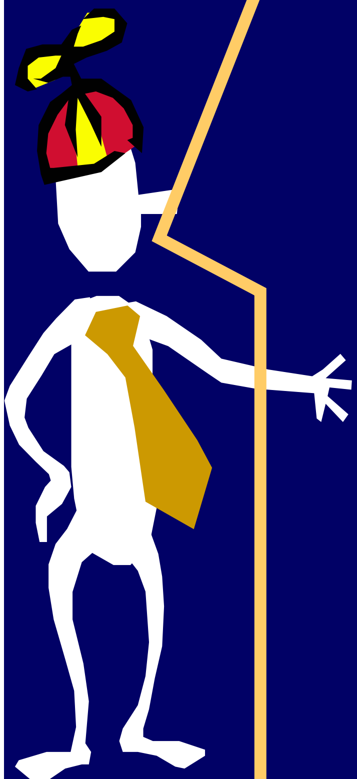
$$a \equiv b \ [\text{mod } n]$$

$$a \equiv_n b$$

"a and b are equivalent modulo n"

iff $(a \text{ mod } n) = (b \text{ mod } n)$

iff $n | (a-b)$



31 equals 81 modulo 2

$$31 \equiv 81 \; [\text{mod } 2]$$

$$31 \equiv_2 81$$

$$(31 \text{ mod } 2) = 1 = (81 \text{ mod } 2)$$

$$2 | (31 - 81)$$

$\equiv_n$ is an equivalence relation

In other words,

Reflexive:

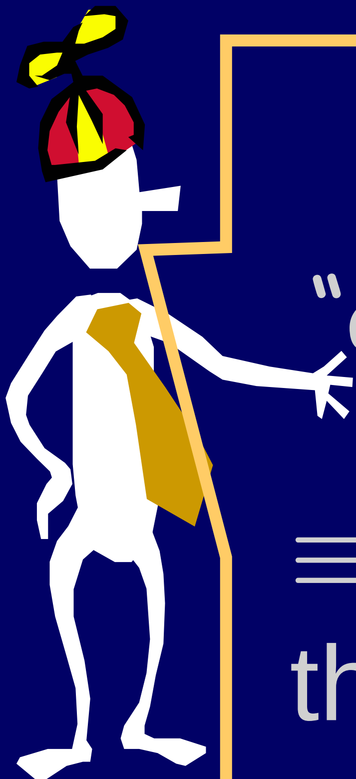
$a \equiv_n a$

Symmetric:

$(a \equiv_n b) \Rightarrow (b \equiv_n a)$

Transitive:

$(a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)$

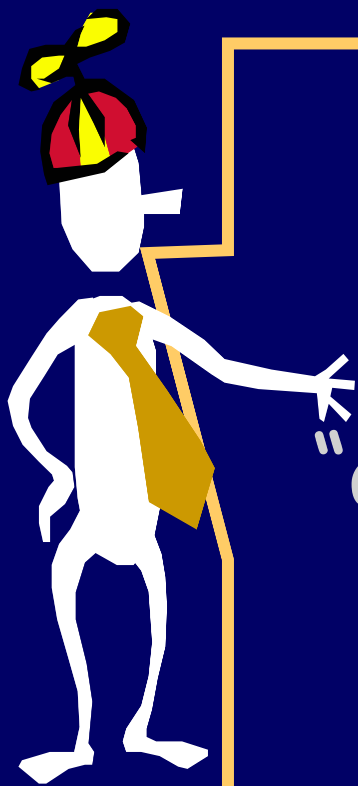


$a \equiv_n b \leftrightarrow n|(a-b)$

"a and b are equivalent modulo n"

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

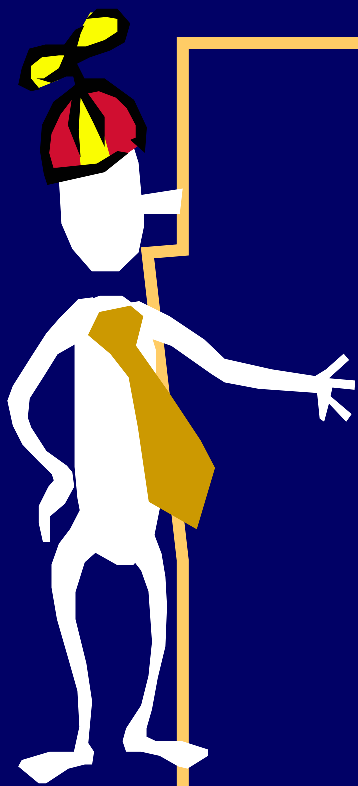
a and b are said to be in the same "residue class" or "congruence class" exactly when $a \equiv_n b$.



$$a \equiv_n b \leftrightarrow n|(a-b)$$

"a and b are equivalent modulo n"

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



Residue Classes Mod 3:

[0] = { …, -6, -3, 0, 3, 6, ..}

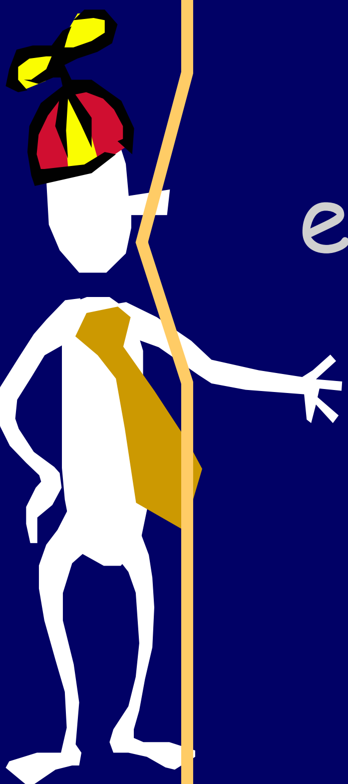
[1] = { …, -5, -2, 1, 4, 7, ..}

[2] = { …, -4, -1, 2, 5, 8, ..}

[-6] = { …, -6, -3, 0, 3, 6, ..}

[7] = { …, -5, -2, 1, 4, 7, ..}

[-1] = { …, -4, -1, 2, 5, 8, ..}



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: $x \equiv_k y$

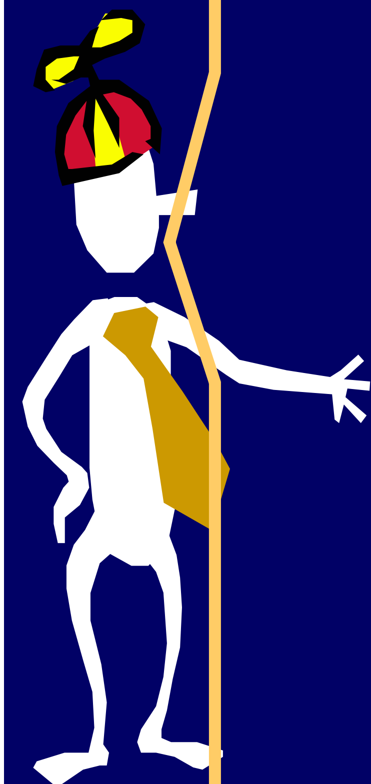
Proof:

Recall, $x \equiv_n y \Leftrightarrow n|(x-y)$

$k|n$ and $n|(x-y)$

Hence, $k|(x-y)$

Of course, $k|(x-y) \Rightarrow x \equiv_k y$



Fundamental lemma of plus, minus, and times modulo n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$

Then: 1) $x+a \equiv_n y+b$

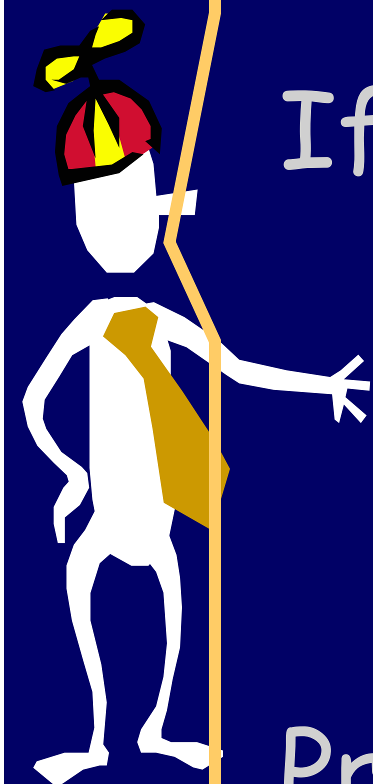
2) $x-a \equiv_n y-b$

3) $xa \equiv_n yb$

Equivalently,

If $n|(x-y)$ and $n|(a-b)$ Then:

1) $n|(x-y + a-b)$
2) $n \mid (x-y - [a-b])$
3) $n|(xa-yb)$



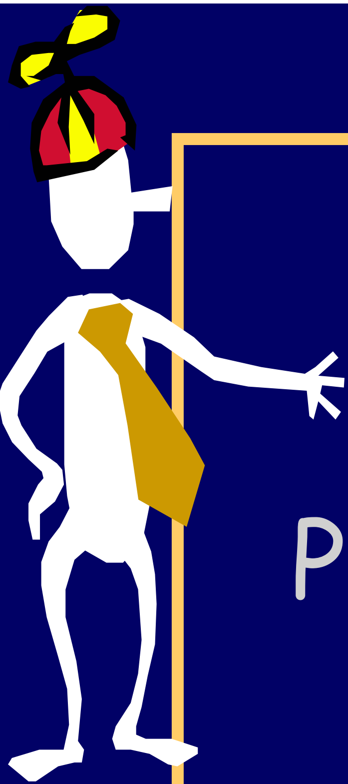
Proof of 3:

$xa-yb = a(x-y) - y(b-a)$

$n|a(x-y)$ and $n|y(b-a)$

Fundamental lemma of plus minus, and times modulo n:

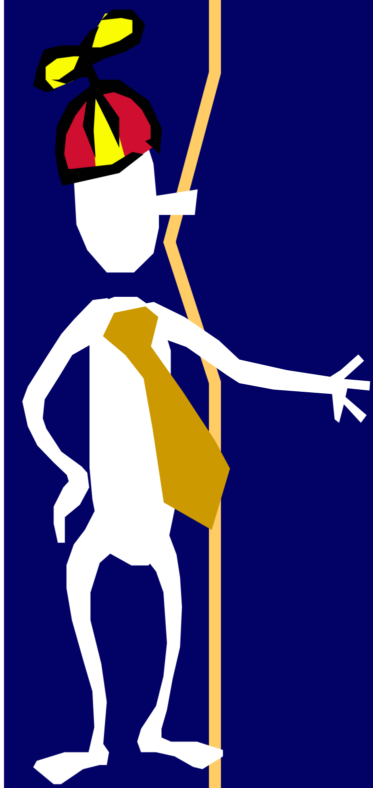
When doing plus, minus, and time modulo n, I can at any time in the calculation replace a number with a number in the same residue class modulo n



Please calculate in your head:

329 * 666 mod 331

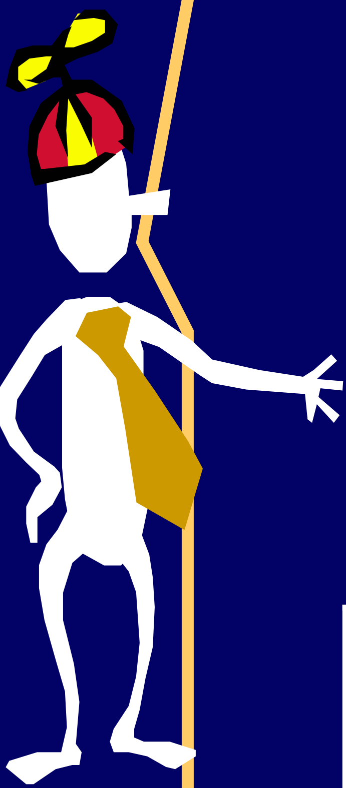
-2 * 4 = -8 = 323



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

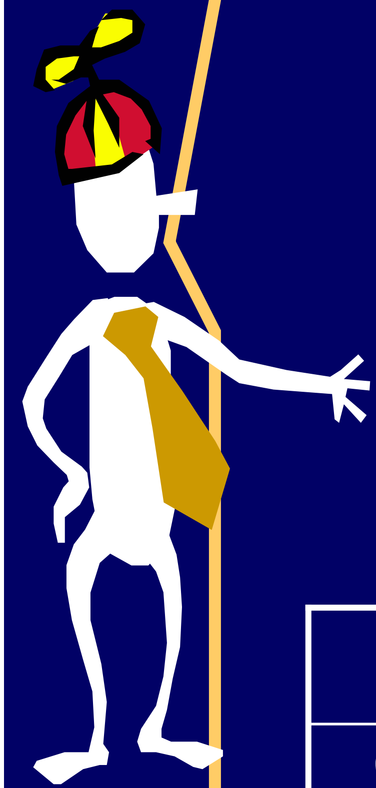


Finite set S = {0, 1, 2}

+ and * defined on S:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1



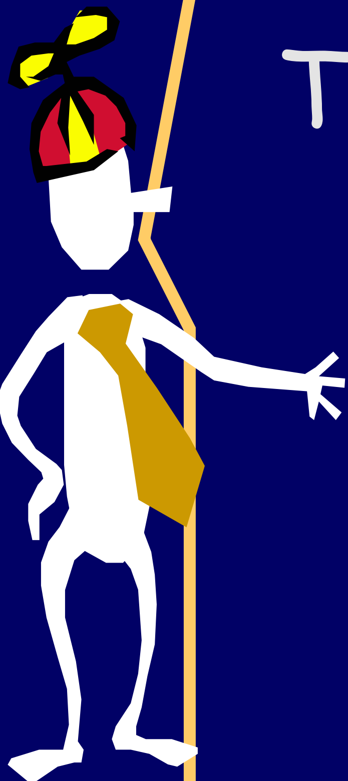
Unique representation system modulo 3

Finite set S = {0, 1, -1}

+ and * defined on S:

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

*	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1



The reduced system modulo n:

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

Define $+_n$ and $*_n$:

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

$$a *_n b = (a*b \bmod n)$$

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

$$a +_n b = (a+b \bmod n) \qquad a *_n b = (a*b \bmod n)$$

$+_n$ and $*_n$ are associative binary operators from $Z_n \times Z_n \to Z_n$:

When $\heartsuit = +_n$ or $*_n$:

[Closure] $x,y \in Z_n \Rightarrow x \heartsuit y \in Z_n$

[Associativity]

$$x,y,z \in Z_n \Rightarrow (x \heartsuit y) \heartsuit z = x \heartsuit (y \heartsuit z)$$

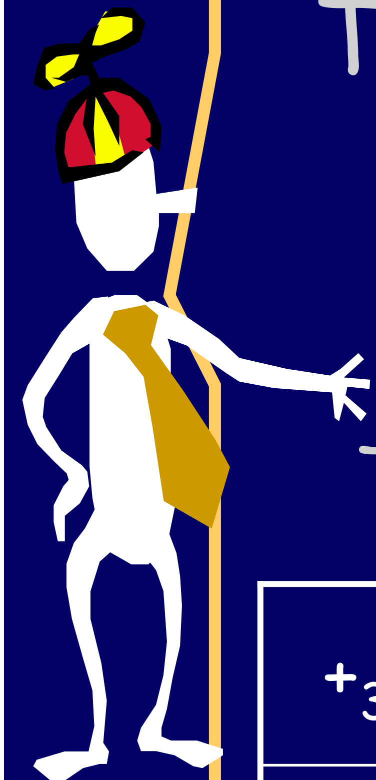
$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \bmod n)$ $\quad$ $a *_n b = (a*b \bmod n)$

$+_n$ and $*_n$ are commutative, associative binary operators from $Z_n \times Z_n \to Z_n$:

[Commutativity]

$$x,y \in Z_n \Rightarrow x \heartsuit y = y \heartsuit x$$



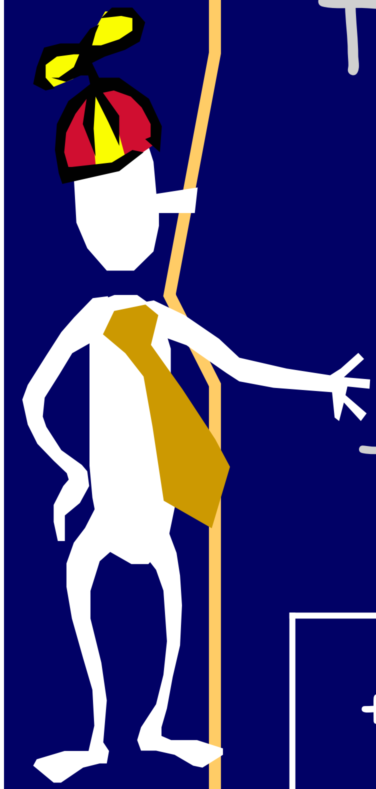
The reduced system modulo 3

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

Two binary, associative operators on Z_3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1



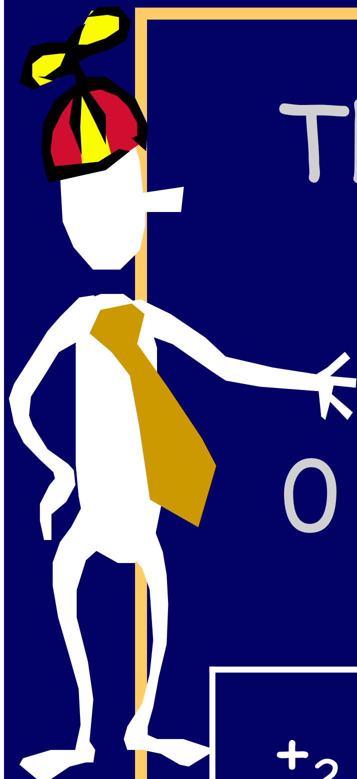
The reduced system modulo 2

$$Z_2 = \{0, 1\}$$

Two binary, associative operators on Z_2:

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

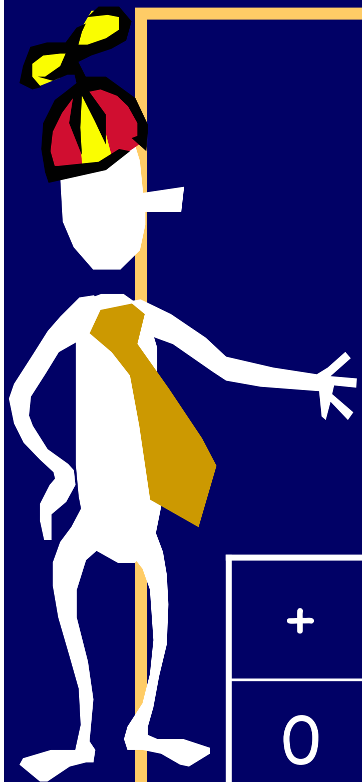


The Boolean interpretation of $Z_2 = \{0, 1\}$

0 means FALSE 1 means TRUE

$+_2$ XOR	0	1
0	0	1
1	1	0

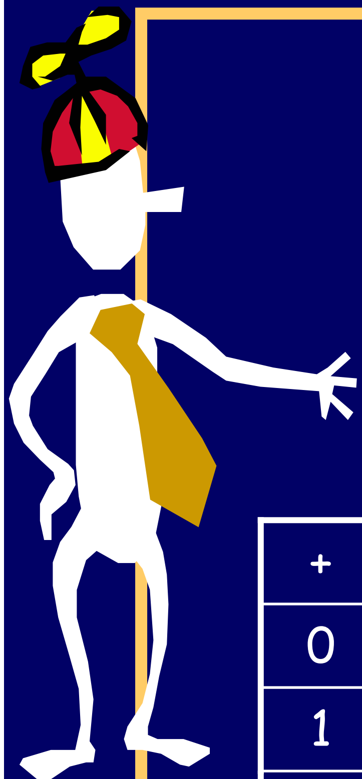
$*_2$ AND	0	1
0	0	0
1	0	1



The reduced system
$Z_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1



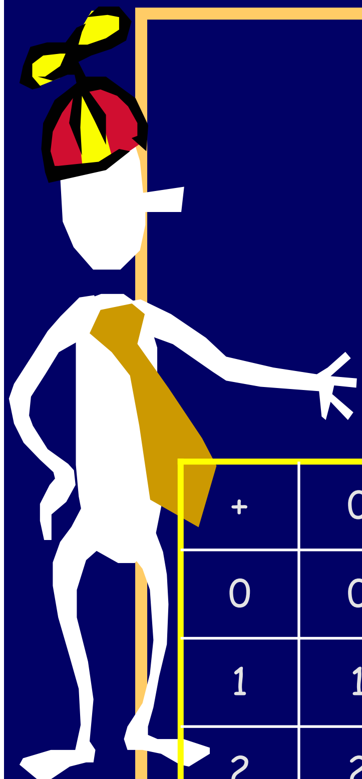
The reduced system
$Z_5 = \{0, 1,2,3,4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	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

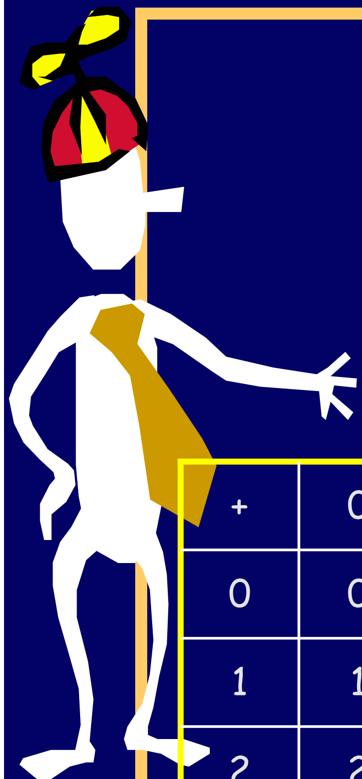
The reduced system

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



+	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

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

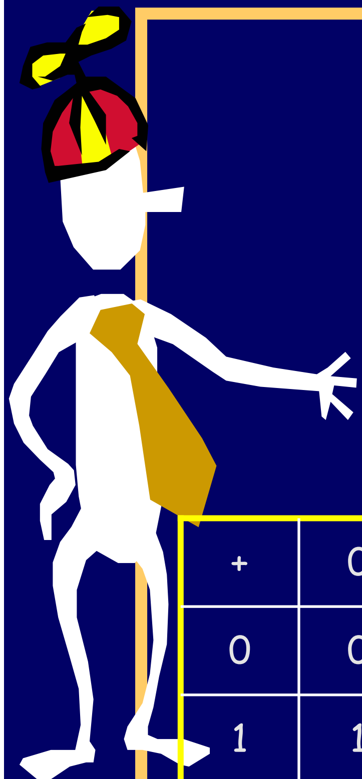


The reduced system

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

+	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

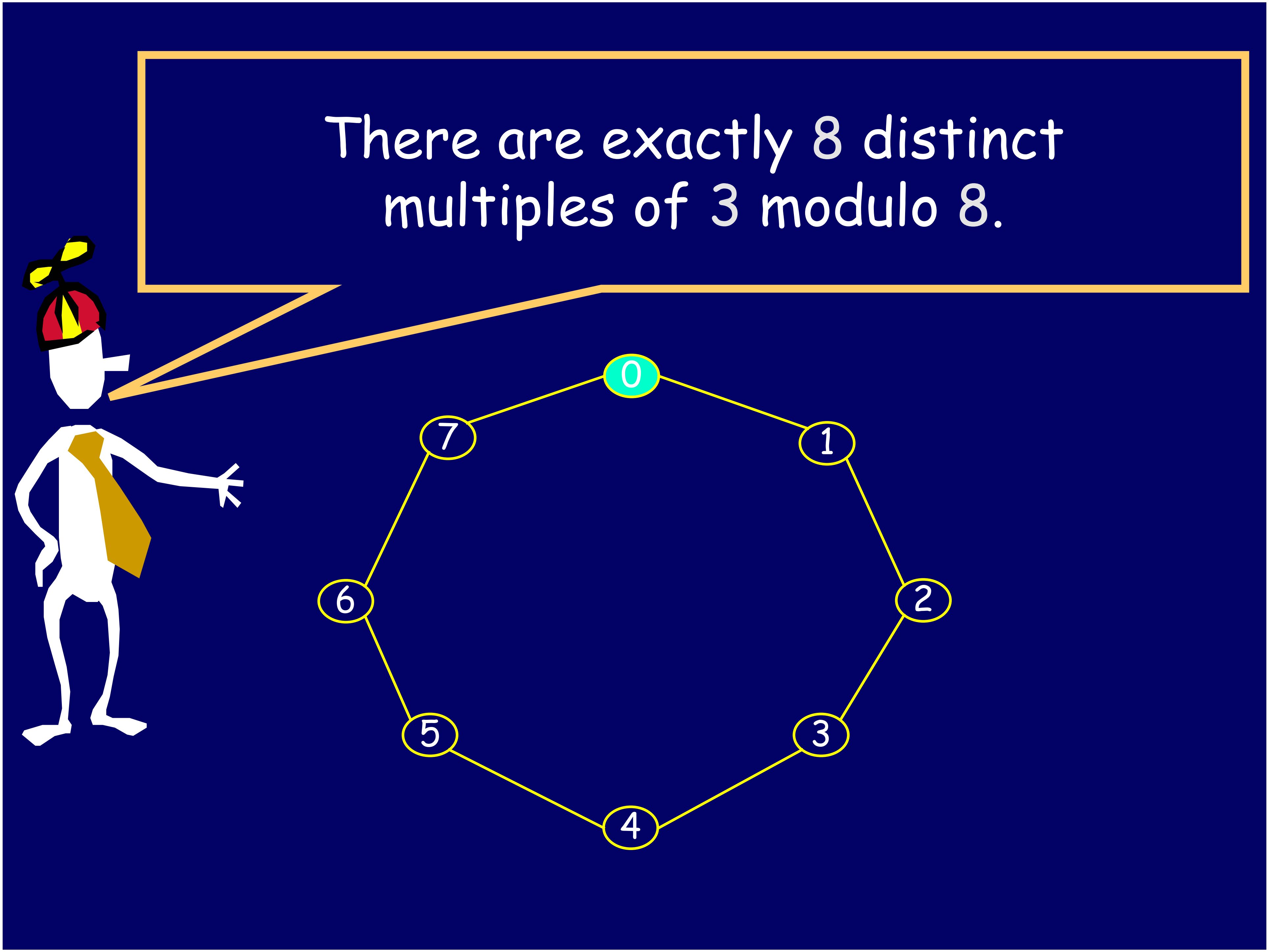
An operator has the permutation property if each row and each column has a permutation of the elements.

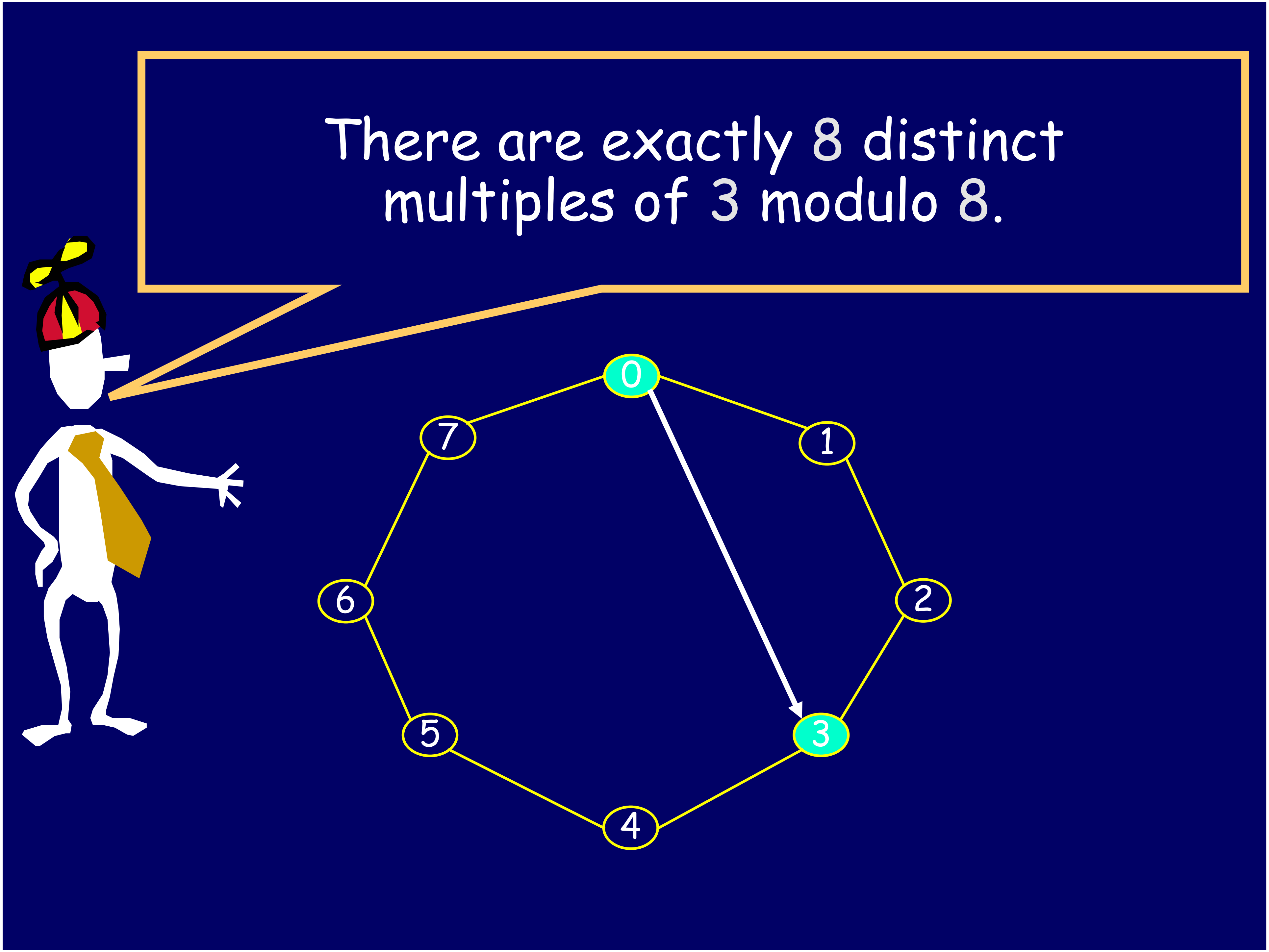


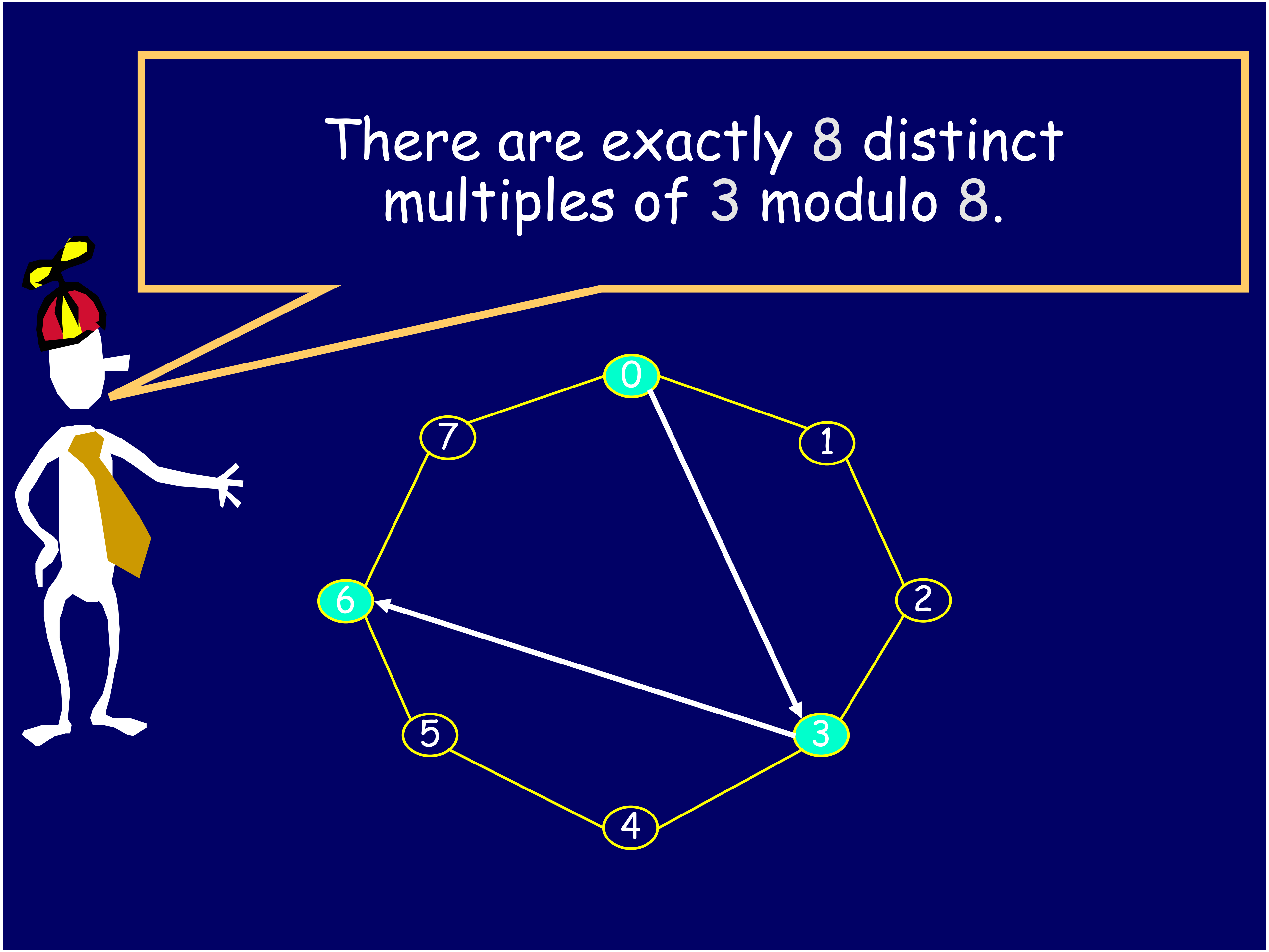
For every n, $+_n$ on Z_n has the permutation property

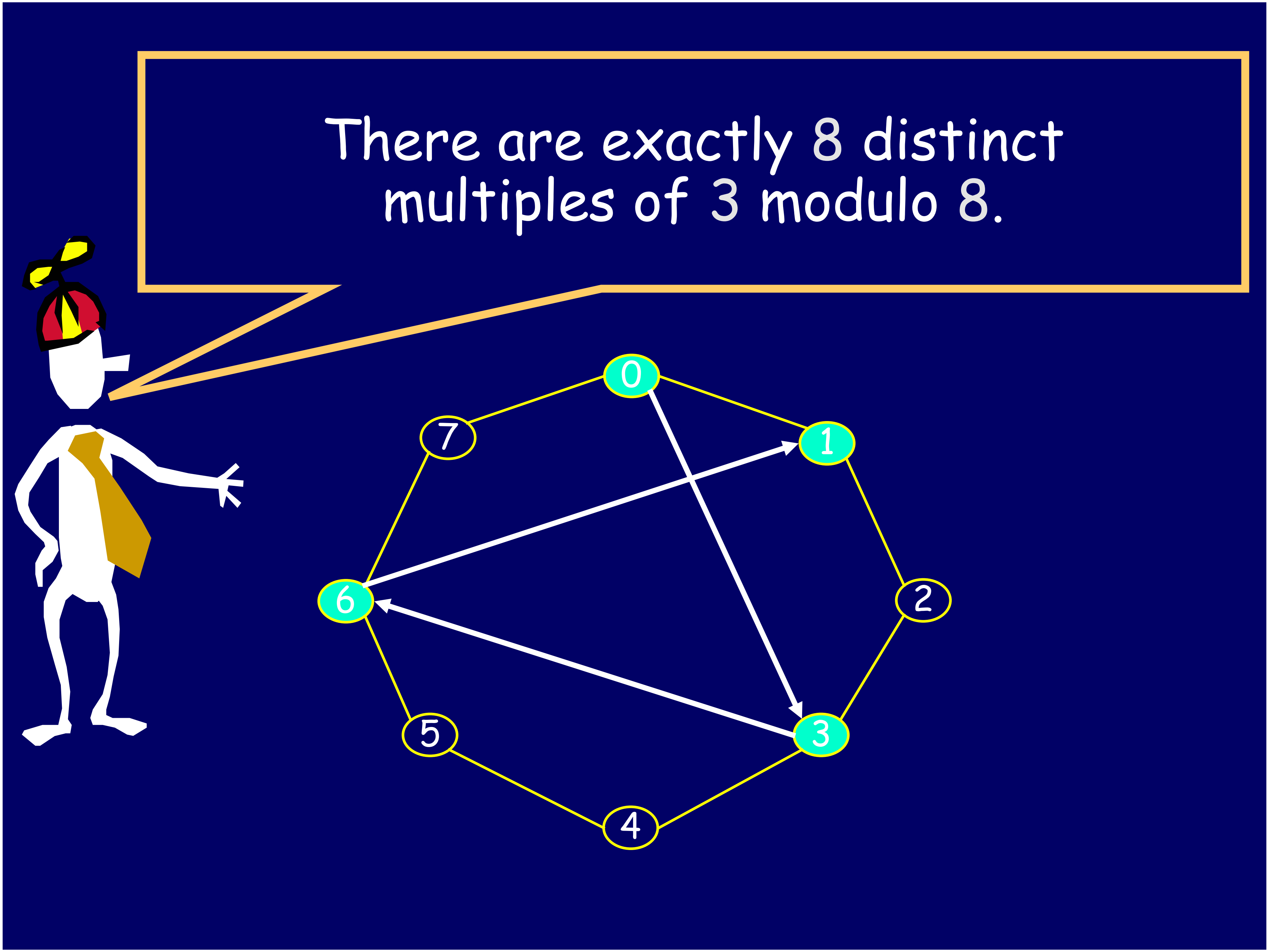
+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

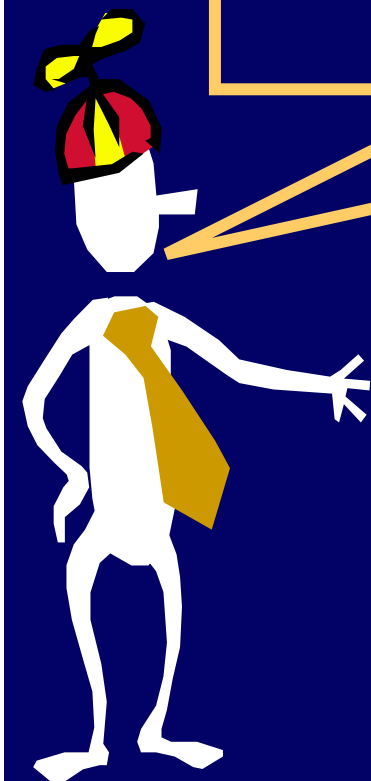
An operator has the permutation property if each row and each column has a permutation of the elements.


There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

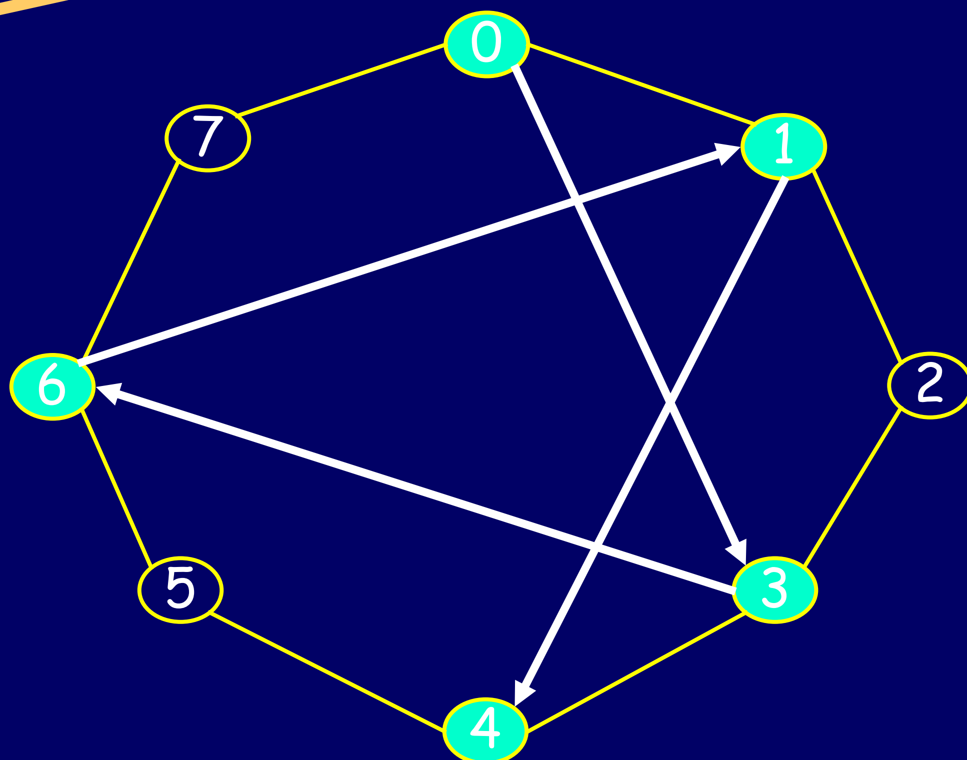

There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

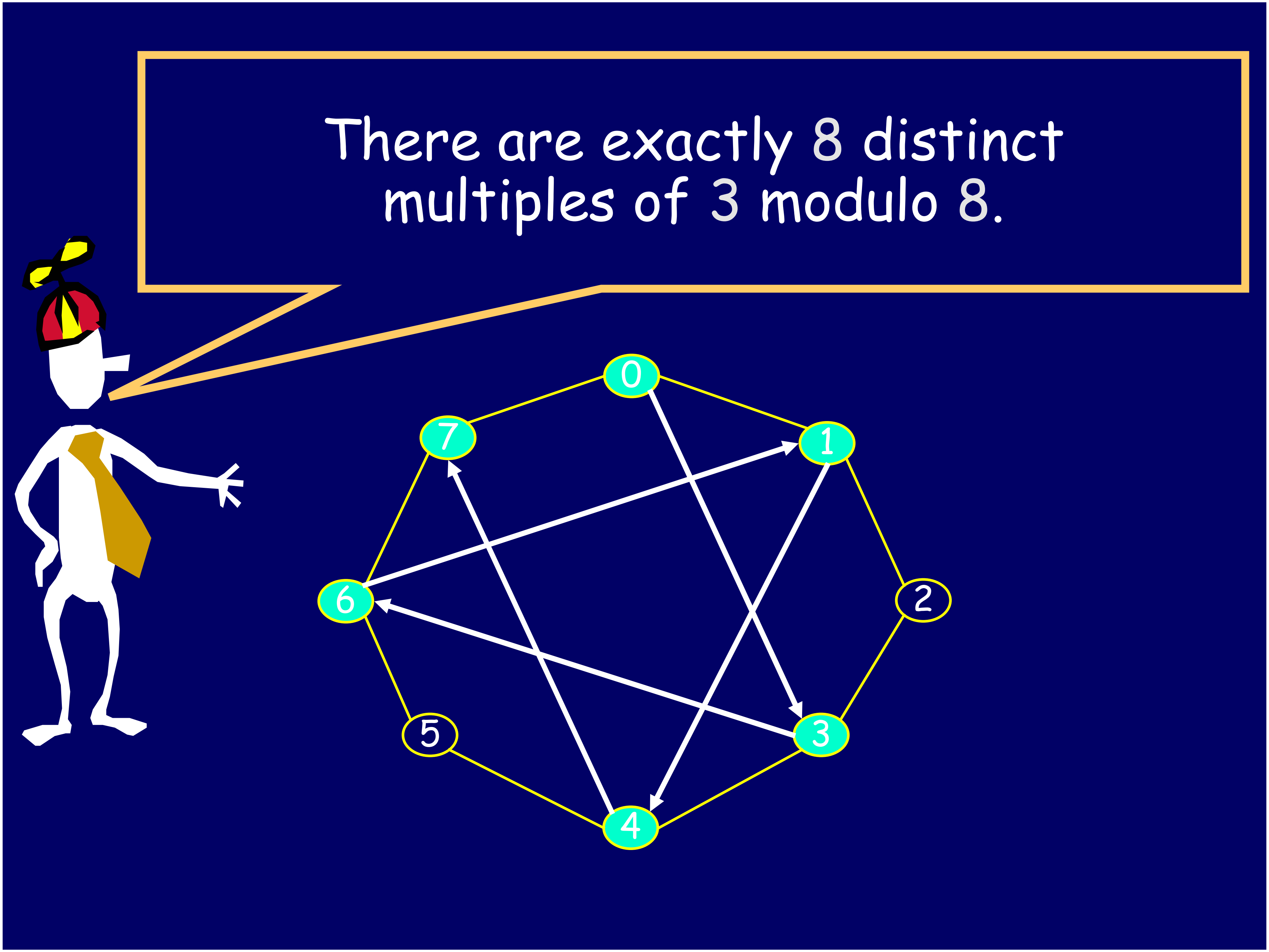

There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

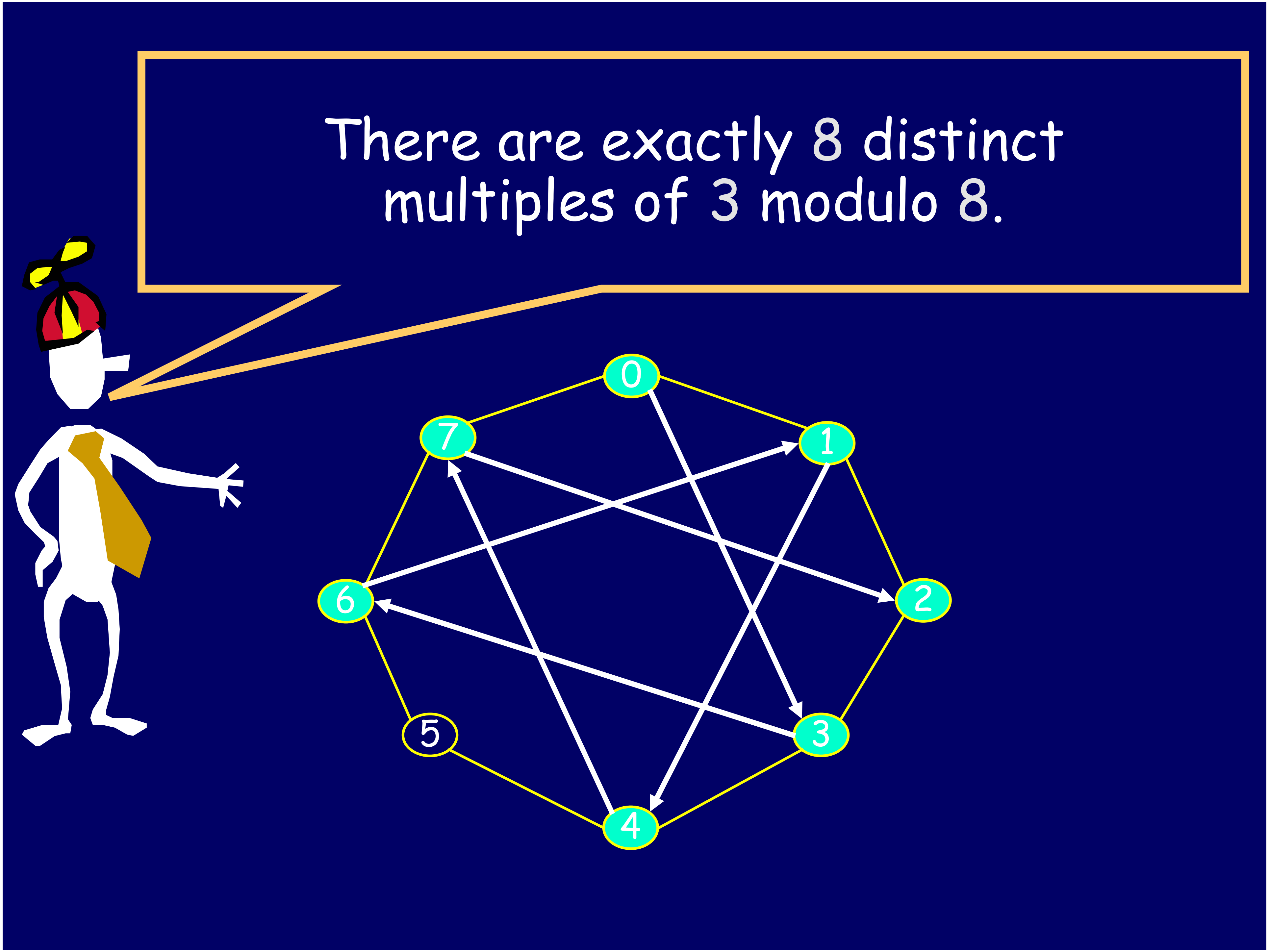

There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

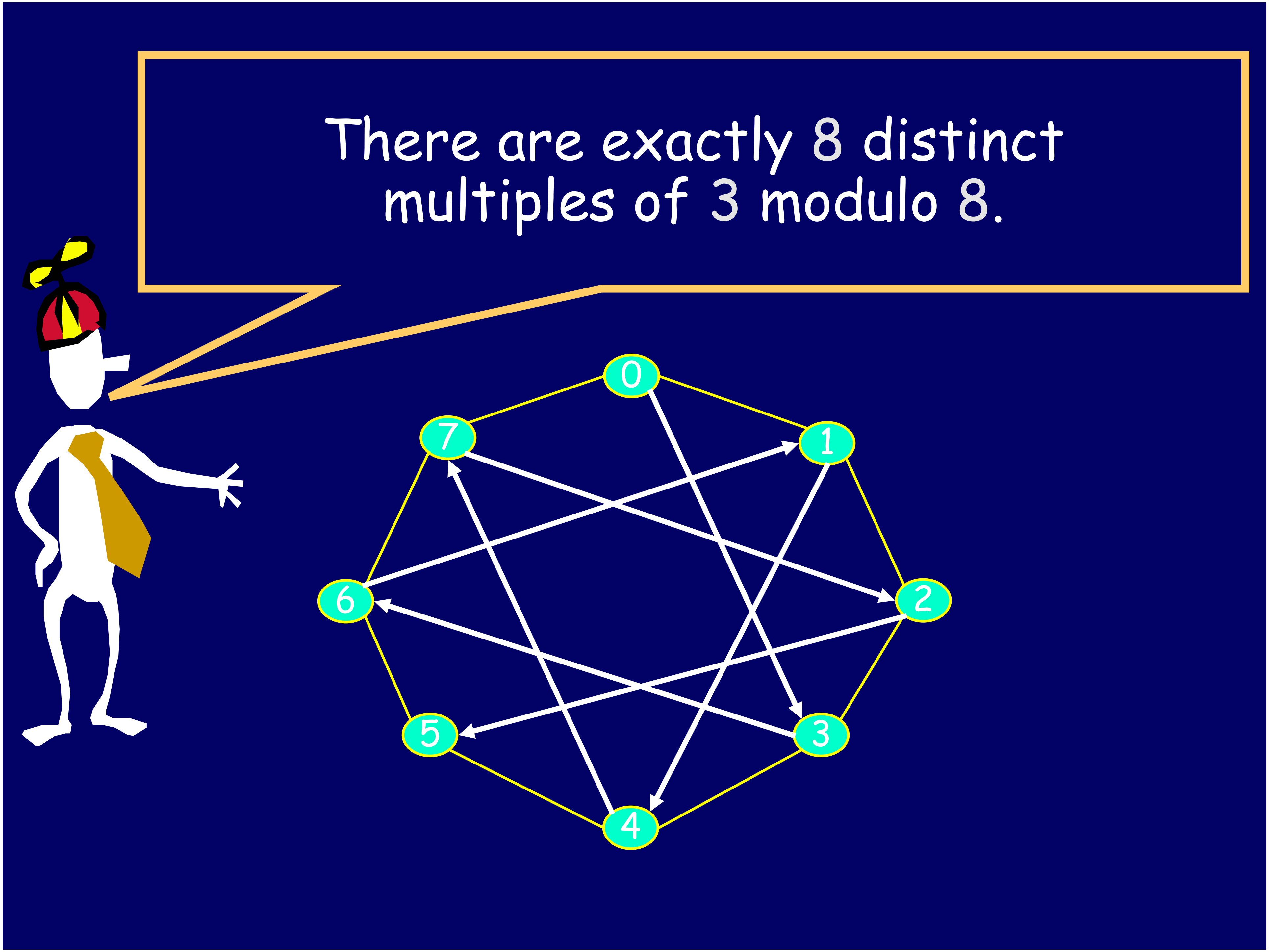


There are exactly 8 distinct multiples of 3 modulo 8..

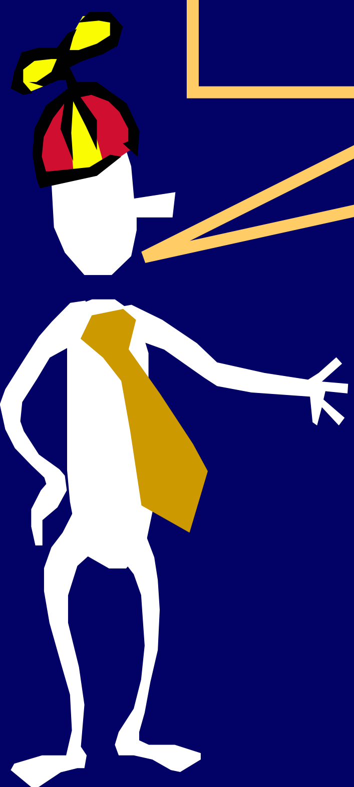


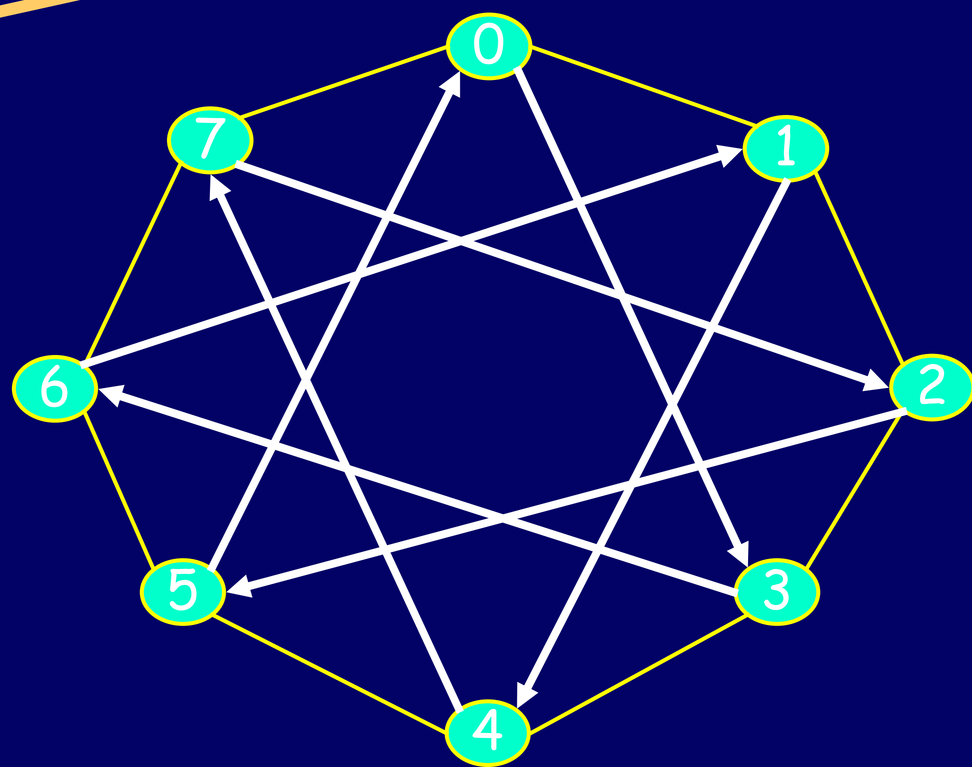

There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7


There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

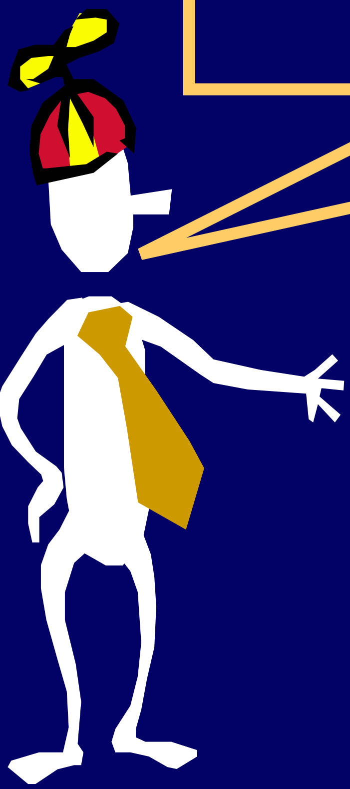

There are exactly 8 distinct multiples of 3 modulo 8.
0
1
2
3
4
5
6
7

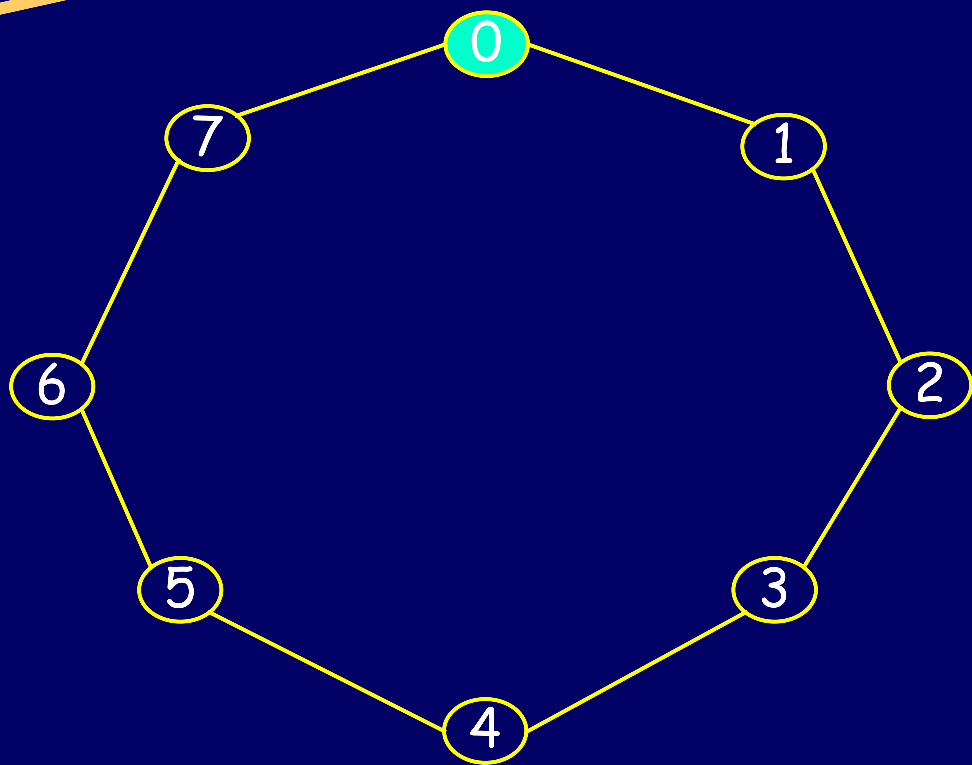
There are exactly 8 distinct multiples of 3 modulo 8.

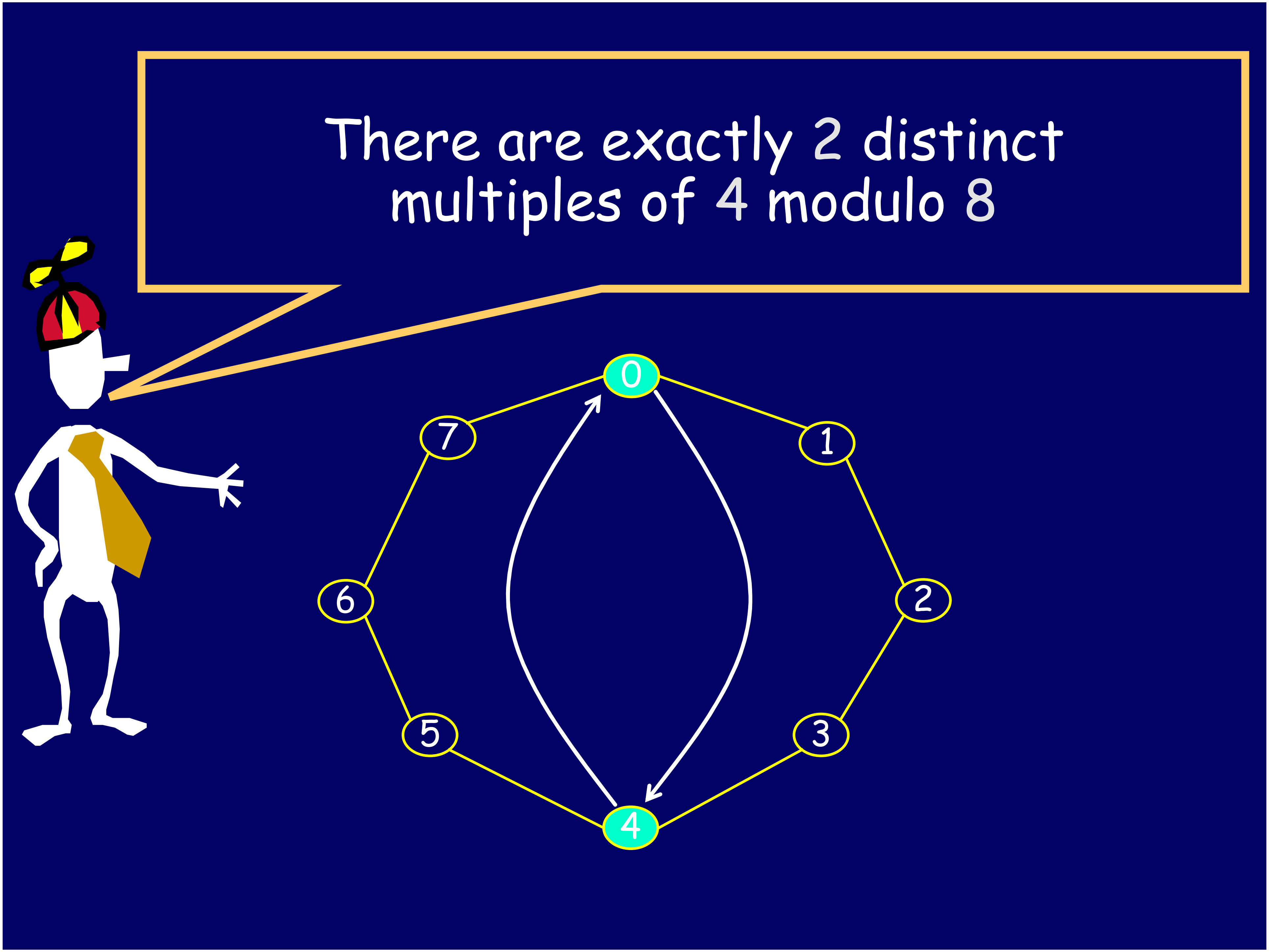




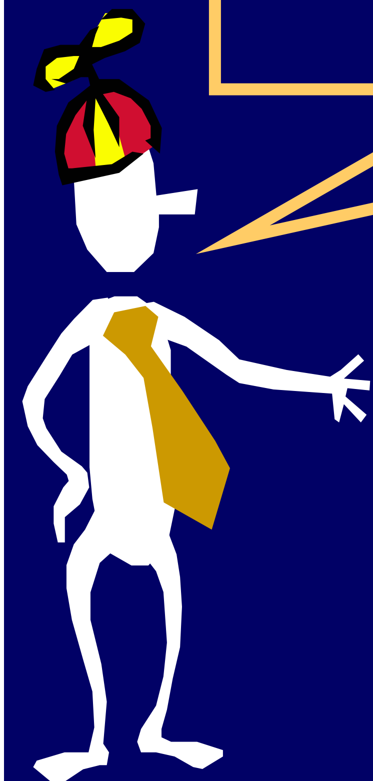
There are exactly 2 distinct multiples of 4 modulo 8.

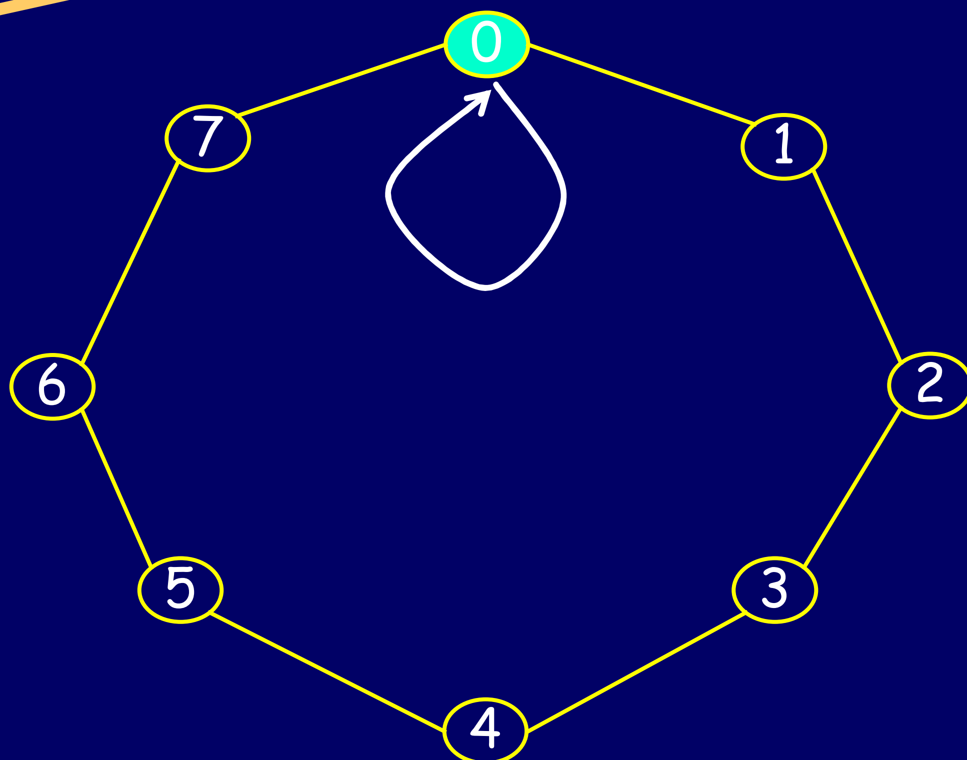


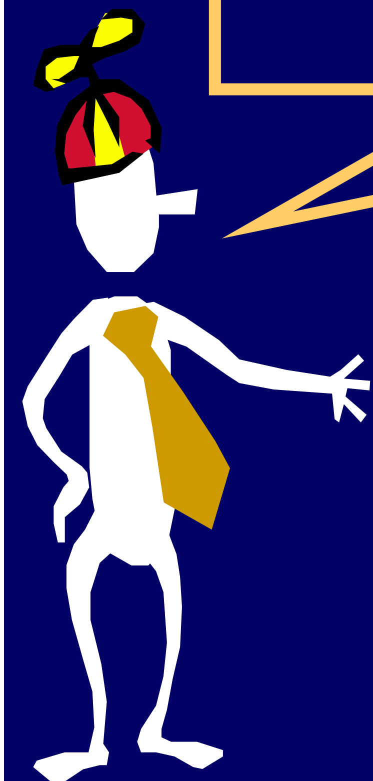



There are exactly 2 distinct
multiples of 4 modulo 8
0
1
2
3
4
5
6
7

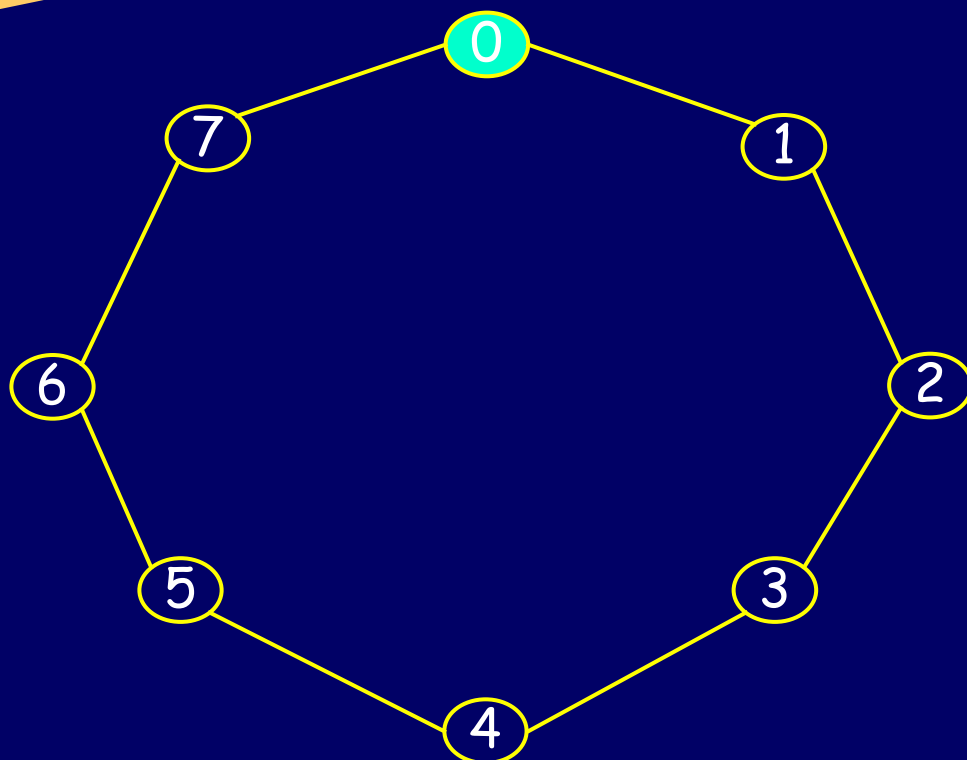
There is exactly 1 distinct multiple of 8 modulo 8

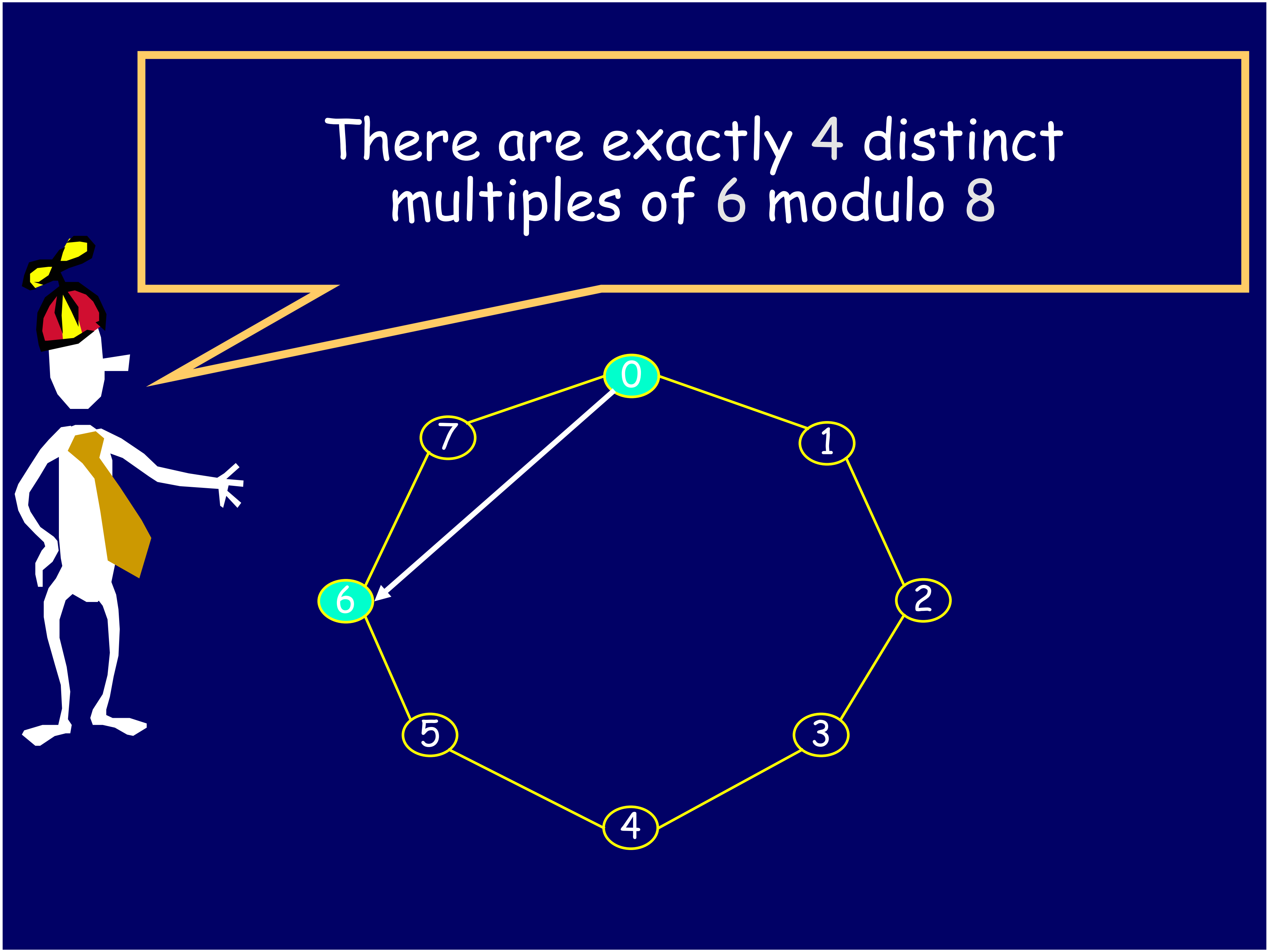


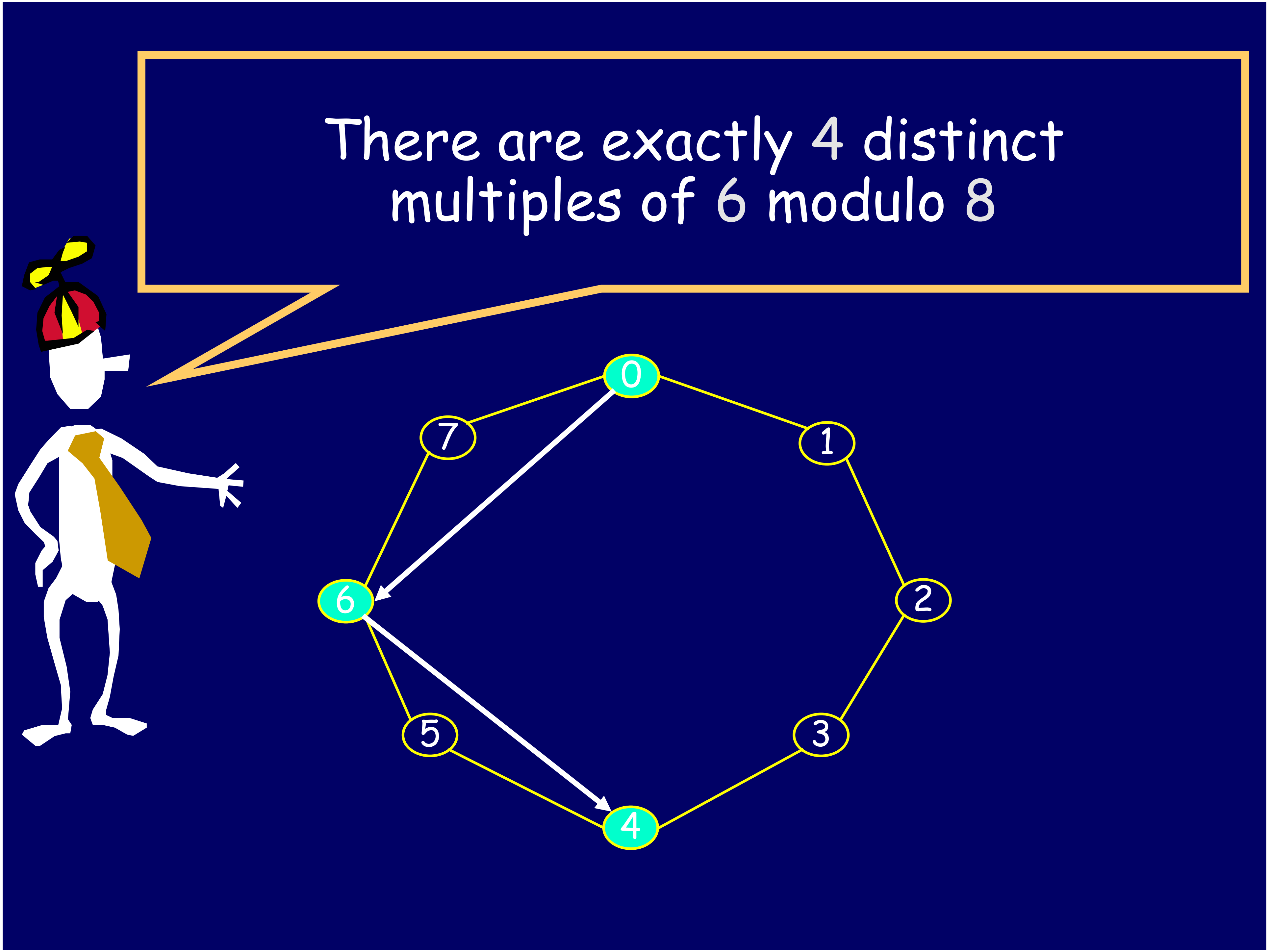


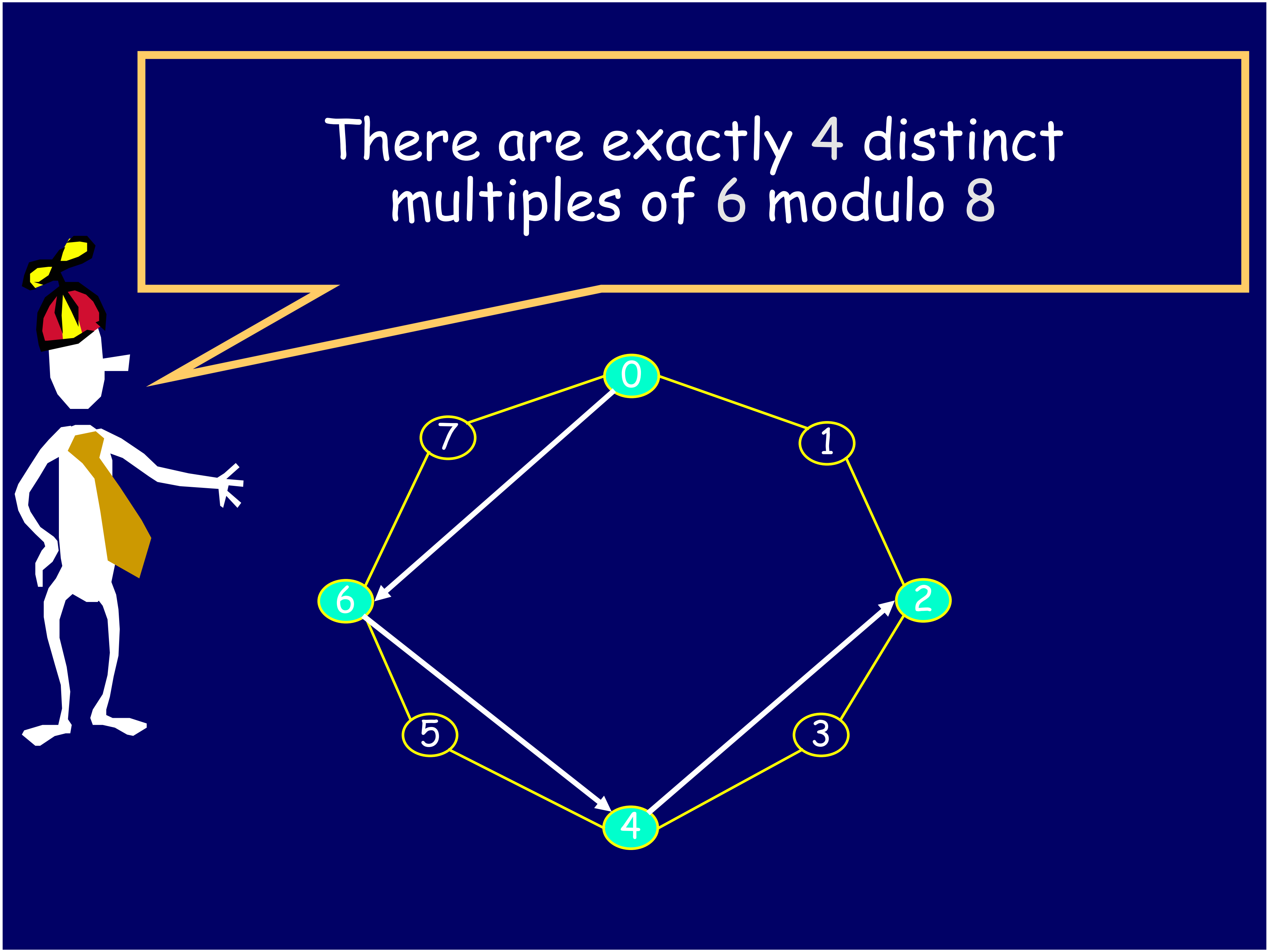


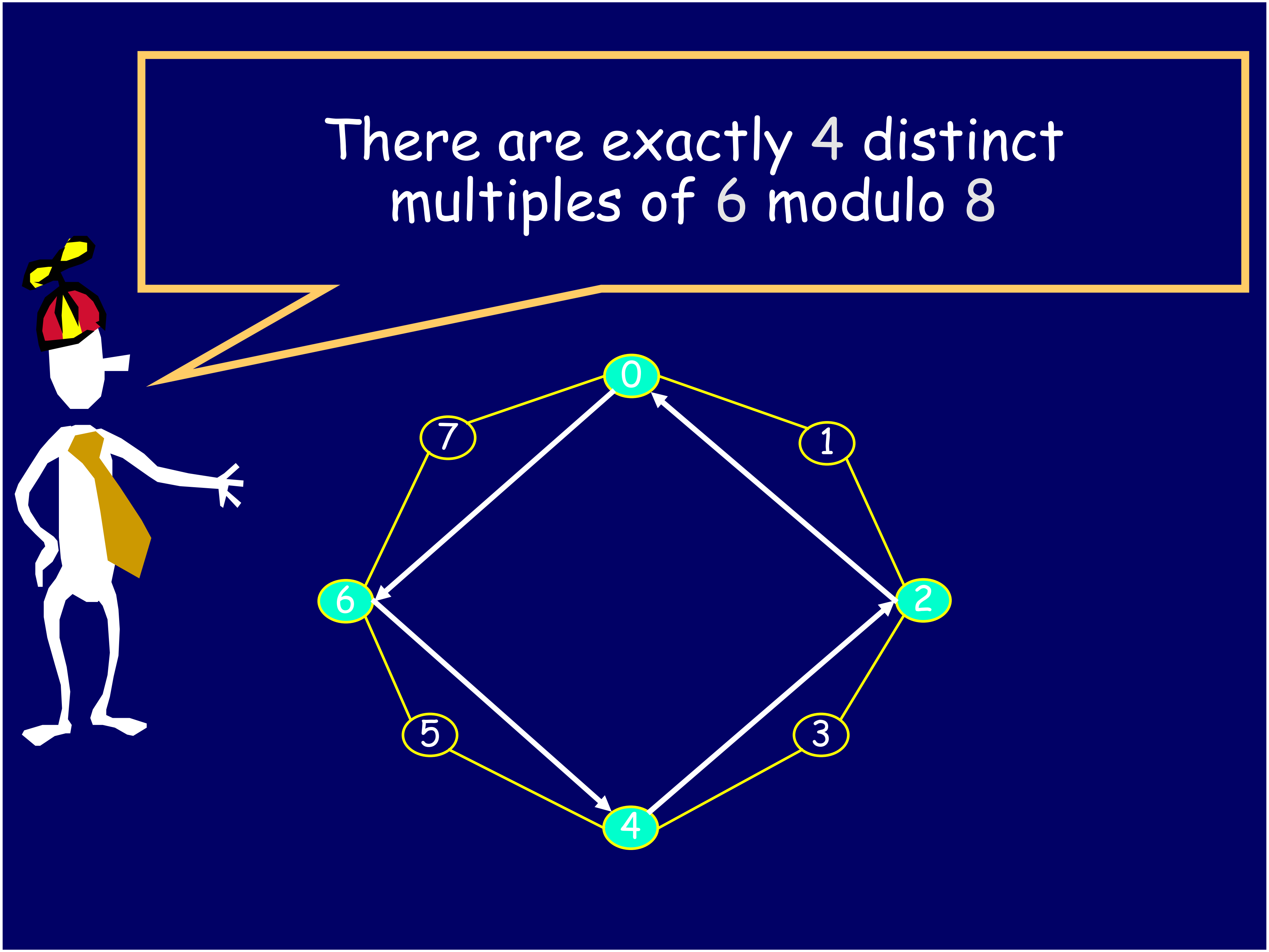
There are exactly 4 distinct multiples of 6 modulo 8



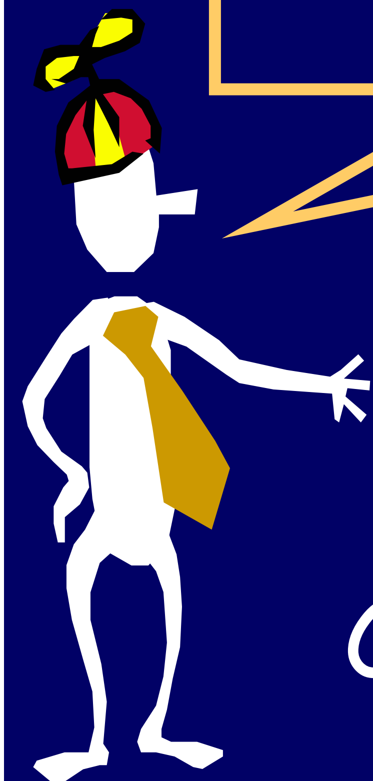

There are exactly 4 distinct multiples of 6 modulo 8
0
1
2
3
4
5
6
7


There are exactly 4 distinct multiples of 6 modulo 8
0
1
2
3
4
5
6
7


There are exactly 4 distinct multiples of 6 modulo 8
0
1
2
3
4
5
6
7

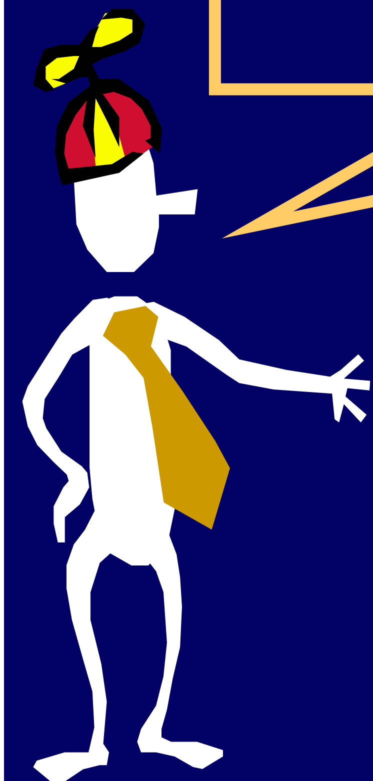

There are exactly 4 distinct multiples of 6 modulo 8
0
1
2
3
4
5
6
7

There are exactly ? distinct multiples of ? modulo ?



Can you see the general rule?

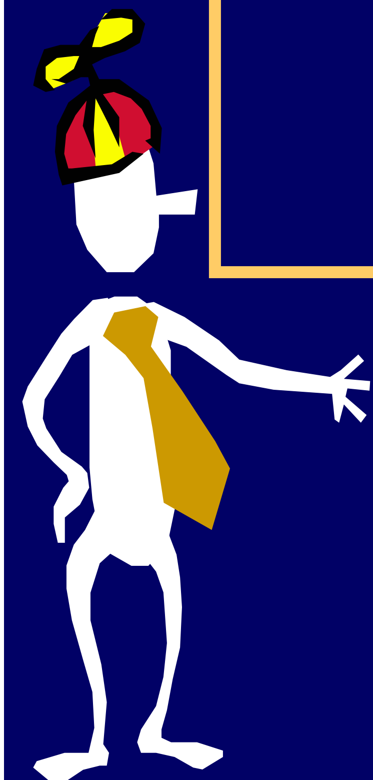
There are exactly n/GCD(c,n) distinct multiples of c modulo n

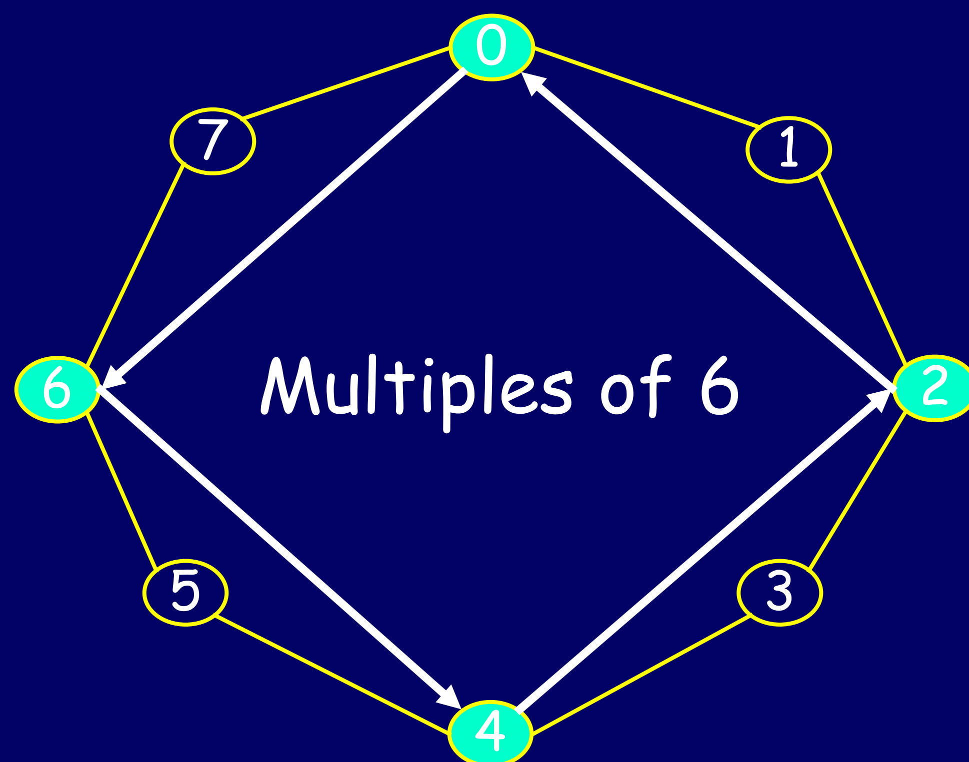


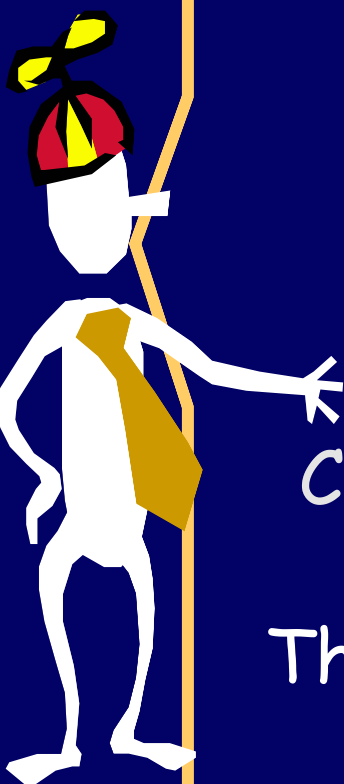
The <u>multiples of c modulo n</u> is the set:

$\{0, c, c +_n c, c +_n c +_n c, \ldots\}$

$= \{kc \bmod n \mid 0 \le k \le n-1\}$







Theorem: There are exactly

$k = n/GCD(c.n)$

distinct multiples of c modulo n:

$\{ c{*}i \bmod n \mid 0 \leq i < k \}$

Clearly, $c/GCD(c,n) \geq 1$ is a whole number

$ck = n\,[c/GCD(c,n)] \equiv_n 0$

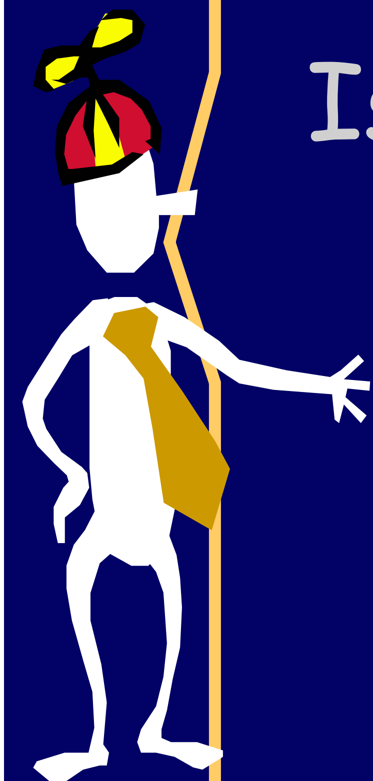
There are $\leq k$ distinct multiples of c mod n:

$c{*}0, c{*}1, c{*}2, \ldots, c{*}(k-1)$

k is all the factors of n missing from c

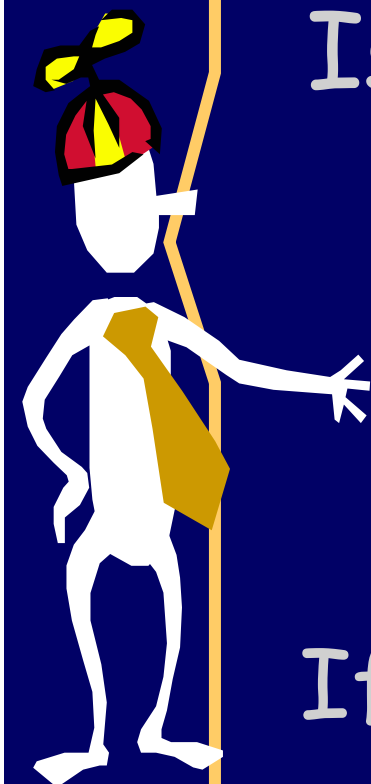
$cx \equiv_n cy \leftrightarrow n|c(x-y) \Rightarrow k|(x-y) \Rightarrow x-y \geq k$

There are $\geq k$ multiples of c



Is there a fundamental lemma of division modulo n?

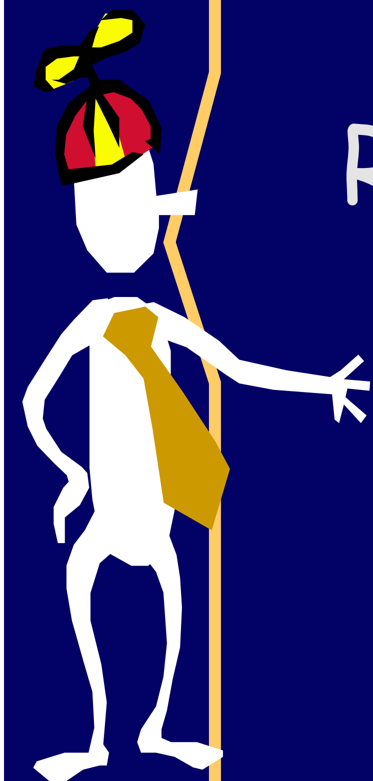
$$cx \equiv_n cy \Rightarrow x \equiv_n y \quad ?$$



Is there a fundamental lemma of division modulo n?

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

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



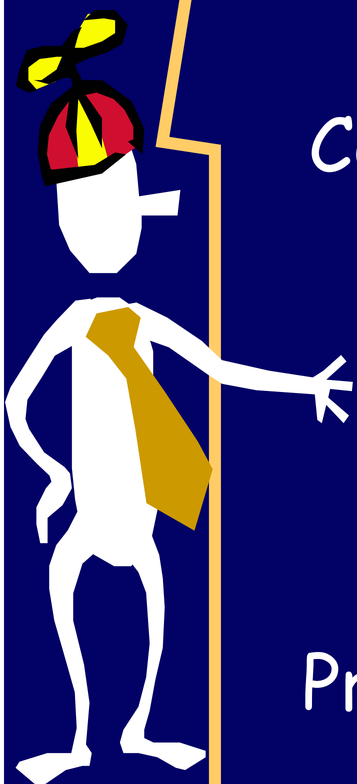
Repaired fundamental lemma of division modulo n?

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

$2*2 \equiv_6 2*5$, but not $2 \equiv_6 5$.

$6*3 \equiv_{10} 6*8$, but not $3 \equiv_{10} 8$.

When can I divide by c?

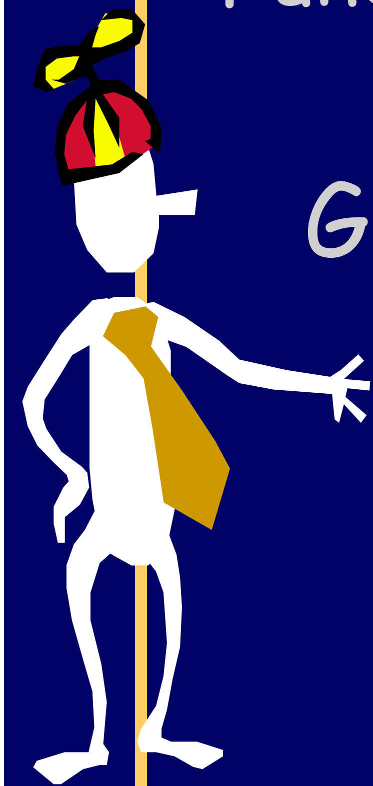


Theorem: There are exactly $n/GCD(c.n)$ distinct multiples of c modulo n.

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 $c*x=c*y$ (but $x \neq y$)



Fundamental lemma of division modulo n.

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

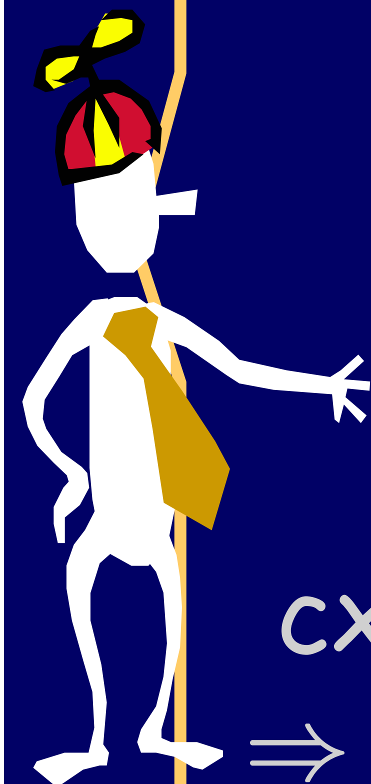
$$ab = ac \bmod n$$

$$n \mid (ab - ac)$$

$$n \mid a(b-c)$$

$$n \mid b-c \qquad \text{since } (a,n)=1$$

$$b = c \bmod n$$



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 $(c, n/_{GCD}(c,n))=1$

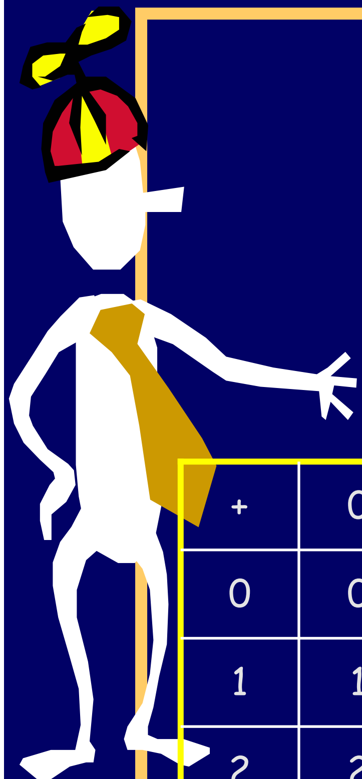
$\Rightarrow x \equiv_{n/(c,n)} y$

Fundamental lemma of division modulo n.

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

$$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$$

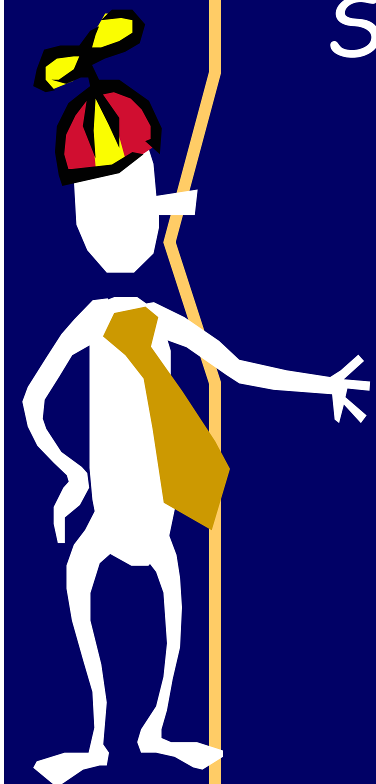
Multiplication over Z_n^* will have the cancellation property.



$$Z_6 = \{0, 1,2,3,4,5\}$$
$$Z_6^* = \{1,5\}$$

+	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

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1



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

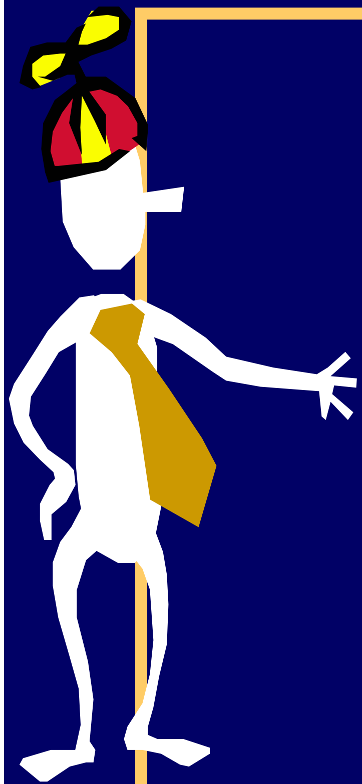
It requires a moment to convince ourselves that GCD(z′,n) =1

$$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$$

$*_n$ is an associative, binary operator. In particular, Z_n^* is closed under $*_n$:

$$x,y \in Z_n^* \Rightarrow x *_n y \in Z_n^* .$$

Proof: Let $z = xy$. Let $z' = z \bmod n$. $z = z' + kn$.
Suppose there exists a prime $p>1$ $p|z'$ and $p|n$.
z is the sum of two multiples of p, so $p|z$.
$p|z \Rightarrow$ that $p|x$ or $p|y$. Contradiction of $x,y \in Z_n^*$

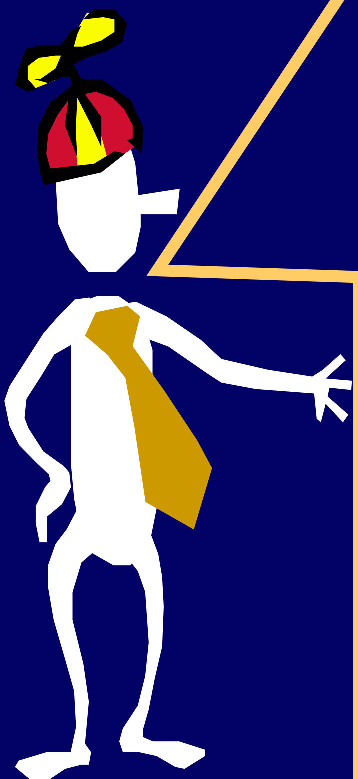


$$Z_{12}^{*} = \{1,5,7,11\}$$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Z_{15}^*

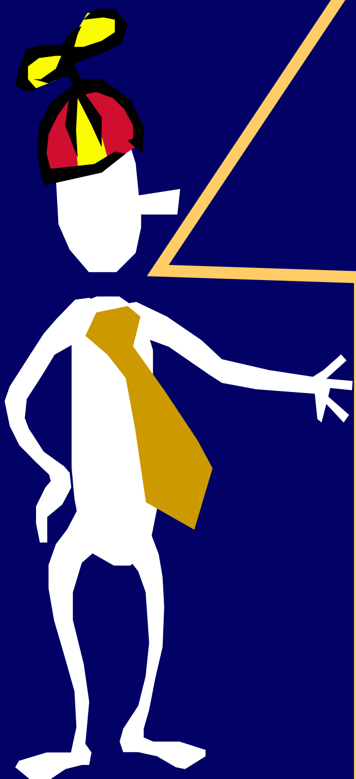
*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1



The column permutation property is equivalent to the right cancellation property:

$$[b * a = c * a] \Rightarrow b=c$$

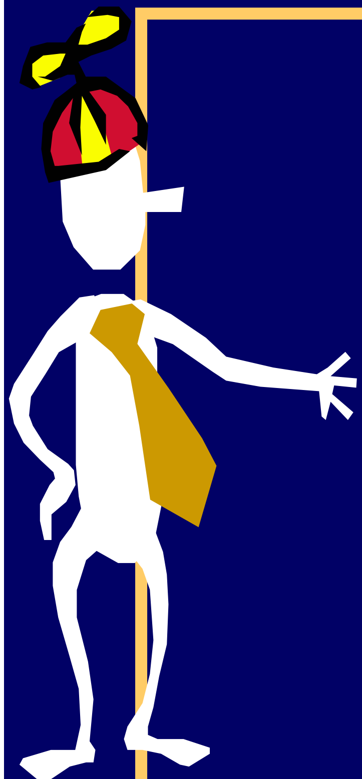
*	1	2	a	4
b	1	2	3	4
2	2	4	1	3
c	3	1	4	2
4	4	3	2	1



The row permutation property is equivalent to the left cancellation property:

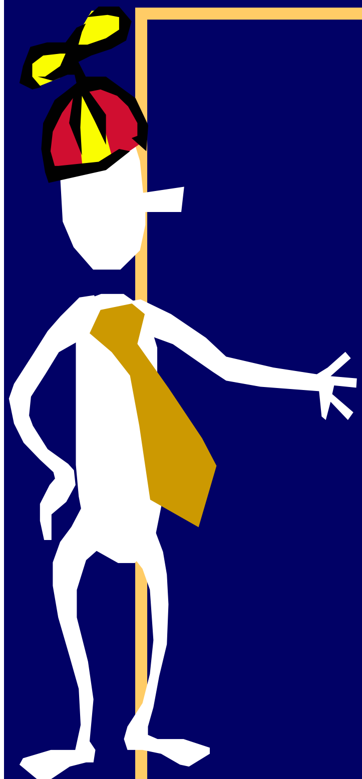
$$[a * b = a * c] \Rightarrow b = c$$

*	b	2	c	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1



$Z_5^* = \{1,2,3,4\}$

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1



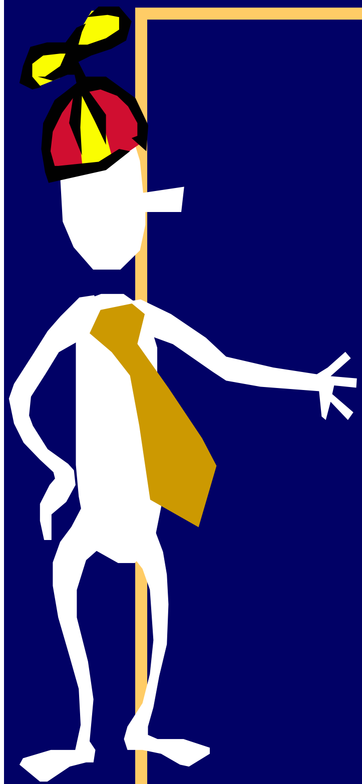
Euler Phi Function

$\Phi(n)$ = size of z_n^*

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

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

$\Rightarrow \Phi(p) = p-1$



$$Z_{12}^{*} = \{1,5,7,11\}$$
$$\phi(12) = 4$$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$$\phi(pq) = (p-1)(q-1)$$

if p,q distinct primes

pq = # of numbers from 1 to pq

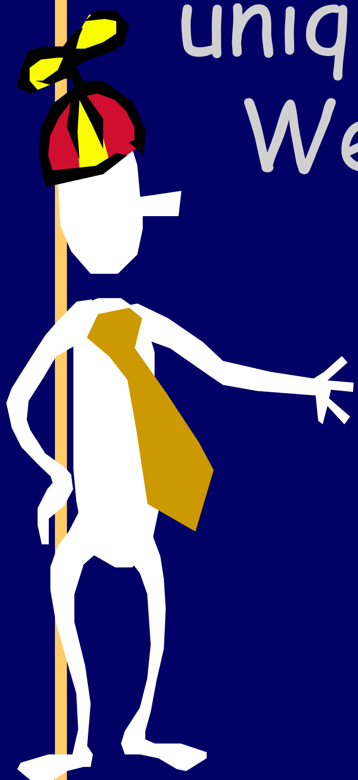
p = # of multiples of q up to pq

q = # of multiples of p up to pq

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

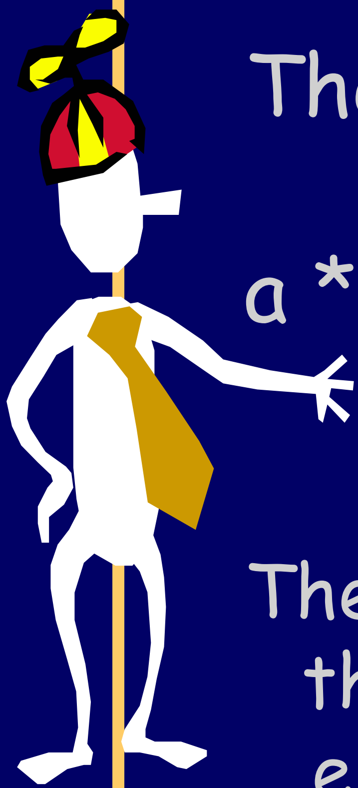
$$\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$$

Let's consider how we do arithmetic in Z_n and in Z_n^*



The additive inverse of $a \in Z_n$ is the unique $b \in Z_n$ such that $a +_n b \equiv_n 0$. We denote this inverse by "$-a$".

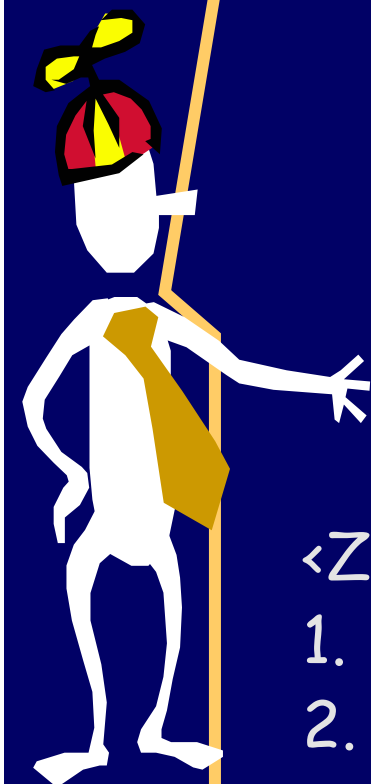
It is trivial to calculate: "$-a$" = $(n-a)$.



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 "$1/a$".

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

*	1	b	3	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1



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

$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

Define $+_n$ and $*_n$:

$a +_n b = (a+b \bmod n)$ $\qquad$ $a *_n b = (a*b \bmod n)$

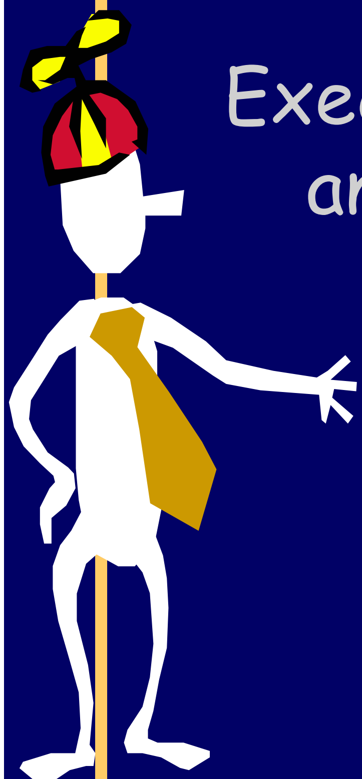
$$c *_n (a +_n b) \equiv_n (c *_n a) +_n (c *_n b)$$

$\langle Z_n, +_n \rangle$

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

$\langle Z_n^*, *_n \rangle$

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 "$1/a$".

<u>Efficient algorithm to compute a^{-1} from a and n.</u>

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:

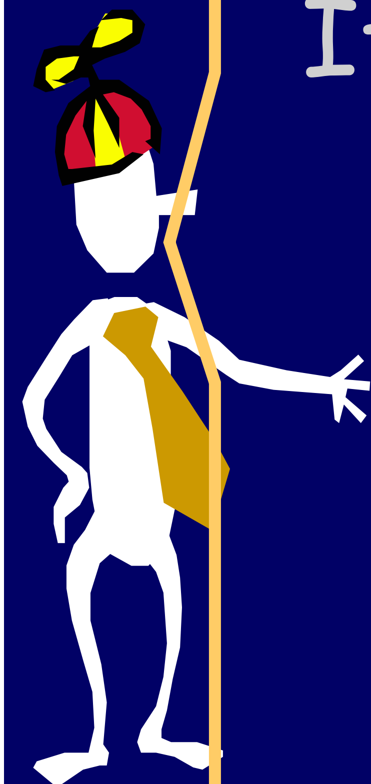
$$rn \equiv_n 1$$

Output r, which is the inverse of a

Fundamental lemma of powers?

If $(a \equiv_n b)$

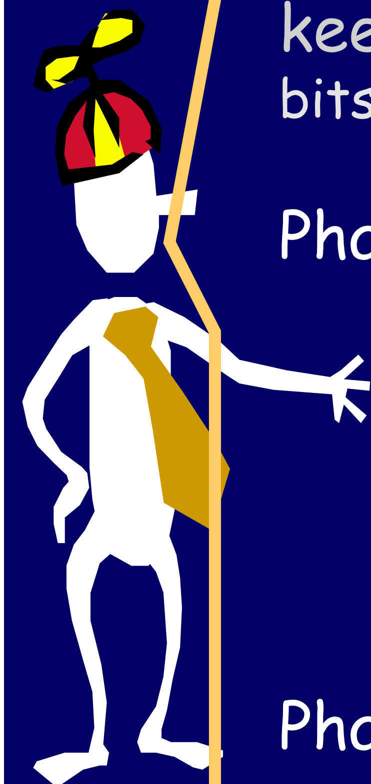
Then $x^a \equiv_n x^b$?



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

NO!

$(16 \equiv_{15} 1)$, 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 $\lfloor \log_2(n) \rfloor + 1$ bits long.

Phase I (Repeated Multiplication)

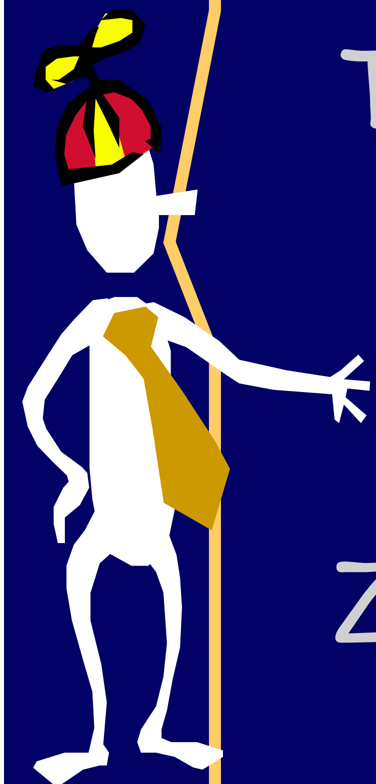
For $\lfloor \log b \rfloor$ steps

multiply largest so far by a

$(a, a^2, a^4, \ldots)$

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:

$$Z_n^* = Z_n^a$$

$$Z_n^a = \{a *_n x \mid x \in Z_n^*\}, \; a \in Z_n^*$$

*	b	2	c	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1

Two products on the same set:

$$Z_n^* = Z_n^a$$

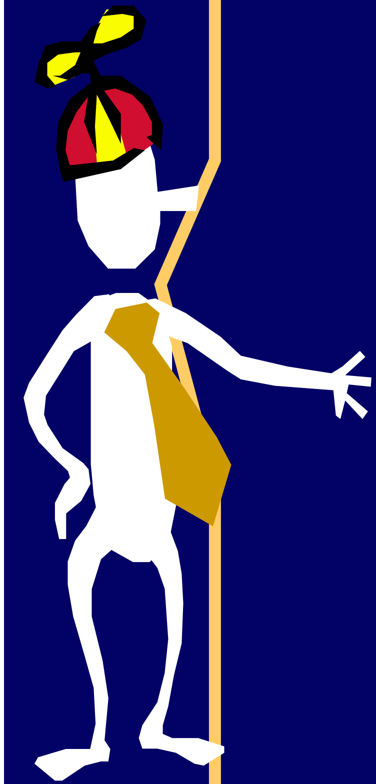
$$Z_n^a = \{a *_n x \mid x \in Z_n^*\},\ a \in Z_n^*$$

$\Pi\, x \equiv_n \Pi\, ax$ [as x ranges over Z_n^*]

$\Pi x \equiv_n \Pi\, x\ (a^{\text{size of } Zn^*})$ [Commutativity]

$1 = a^{\text{size of } Zn^*}$ [Cancellation]

$$a^{\Phi(n)} = 1$$



Euler's Theorem

$$a \in Z_n^*,\ a^{\Phi(n)} \equiv_n 1$$

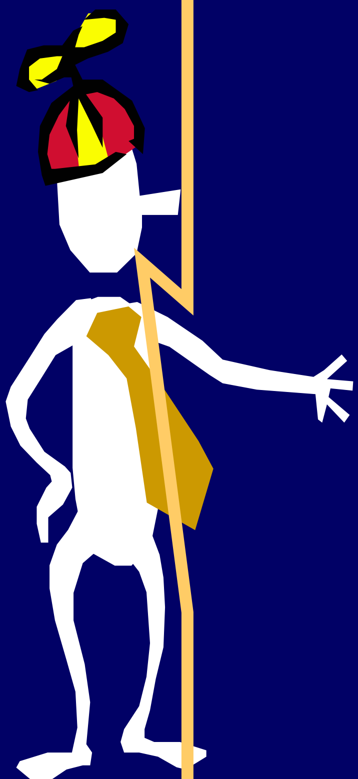
Fermat's Little Theorem

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

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,

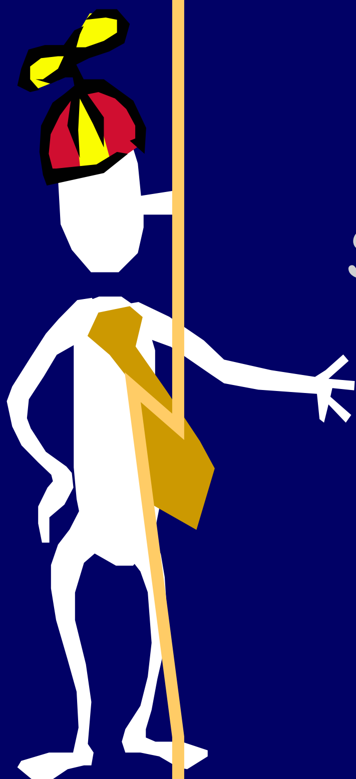
$$x^{a \bmod \Phi(n)} \equiv_n x^{b \bmod \Phi(n)}$$

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.

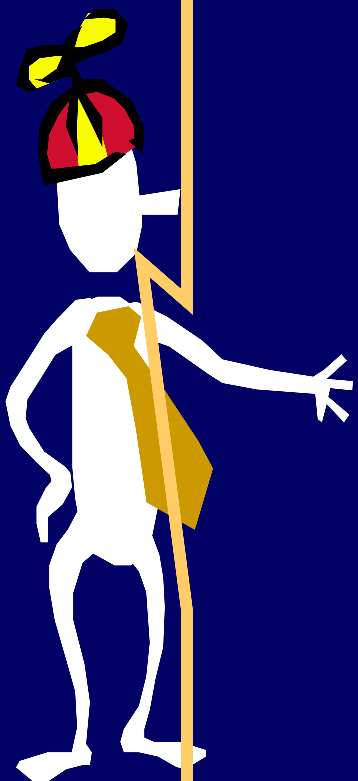
$$(xy)^{-1} \equiv_n x^{-1} y^{-1}$$

$$X^a X^b \equiv_n X^{a+b}$$

Lemma of integer powers.

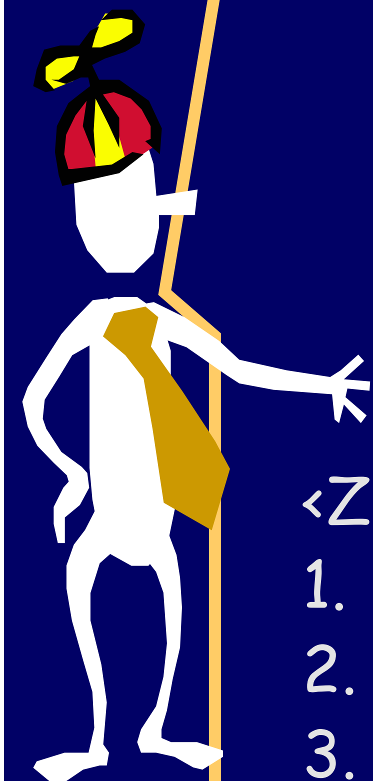
Suppose $x \in Z_n^*$, and a,b are integers.

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



Equivalently,

$$x^{a \bmod \Phi(n)} \equiv_n x^{b \bmod \Phi(n)}$$



$$Z_n = \{0, 1, 2, ..., n-1\}$$
$$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$$

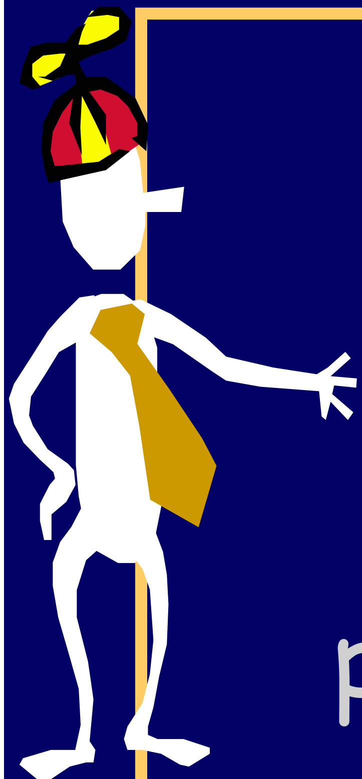
Quick raising to power.

$\langle Z_n, +_n \rangle$

1. Closed
2. Associative
3. 0 is identity
4. Additive Inverses
   Fast + amd -
5. Cancellation
6. Commutative

$\langle Z_n^*, *_n \rangle$

1. Closed
2. Associative
3. 1 is identity
4. Multiplicative Inverses
   Fast * and /
5. Cancellation
6. Commutative



Euler Phi Function

$\Phi(n)$ = size of z_n^*

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

$\Rightarrow \Phi(p) = p-1$

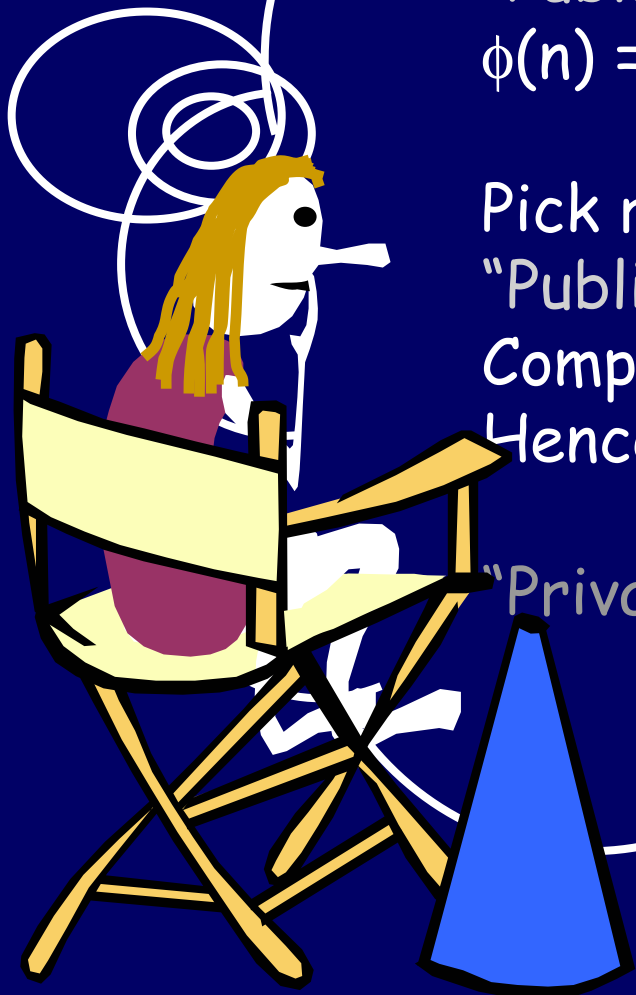
$\phi(pq) = (p-1)(q-1)$

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": $n = p*q$

$\phi(n) = \phi(p)\ \phi(q) = (p-1)*(q-1)$

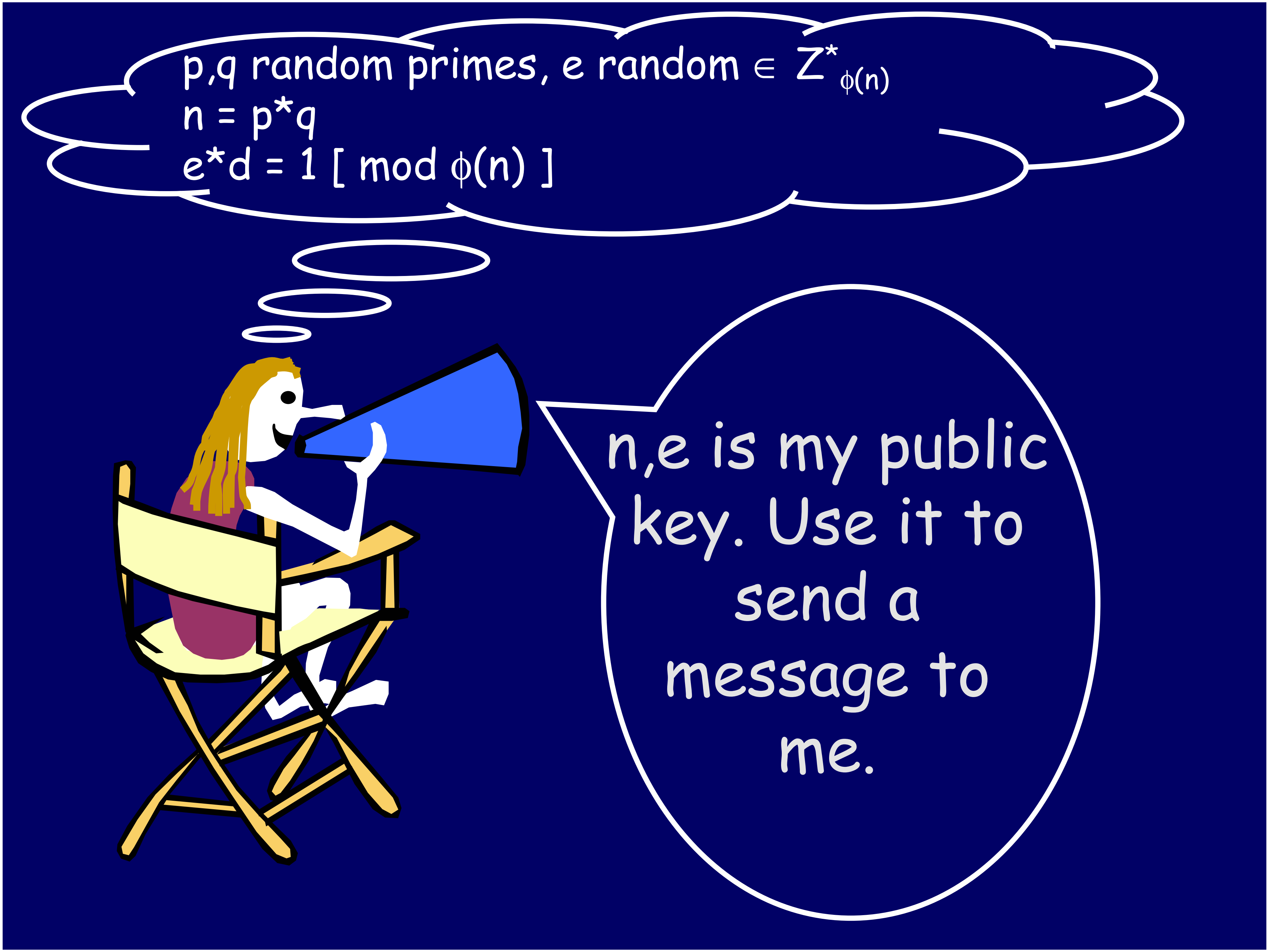
Pick random $e \in Z^*_{\phi(n)}$

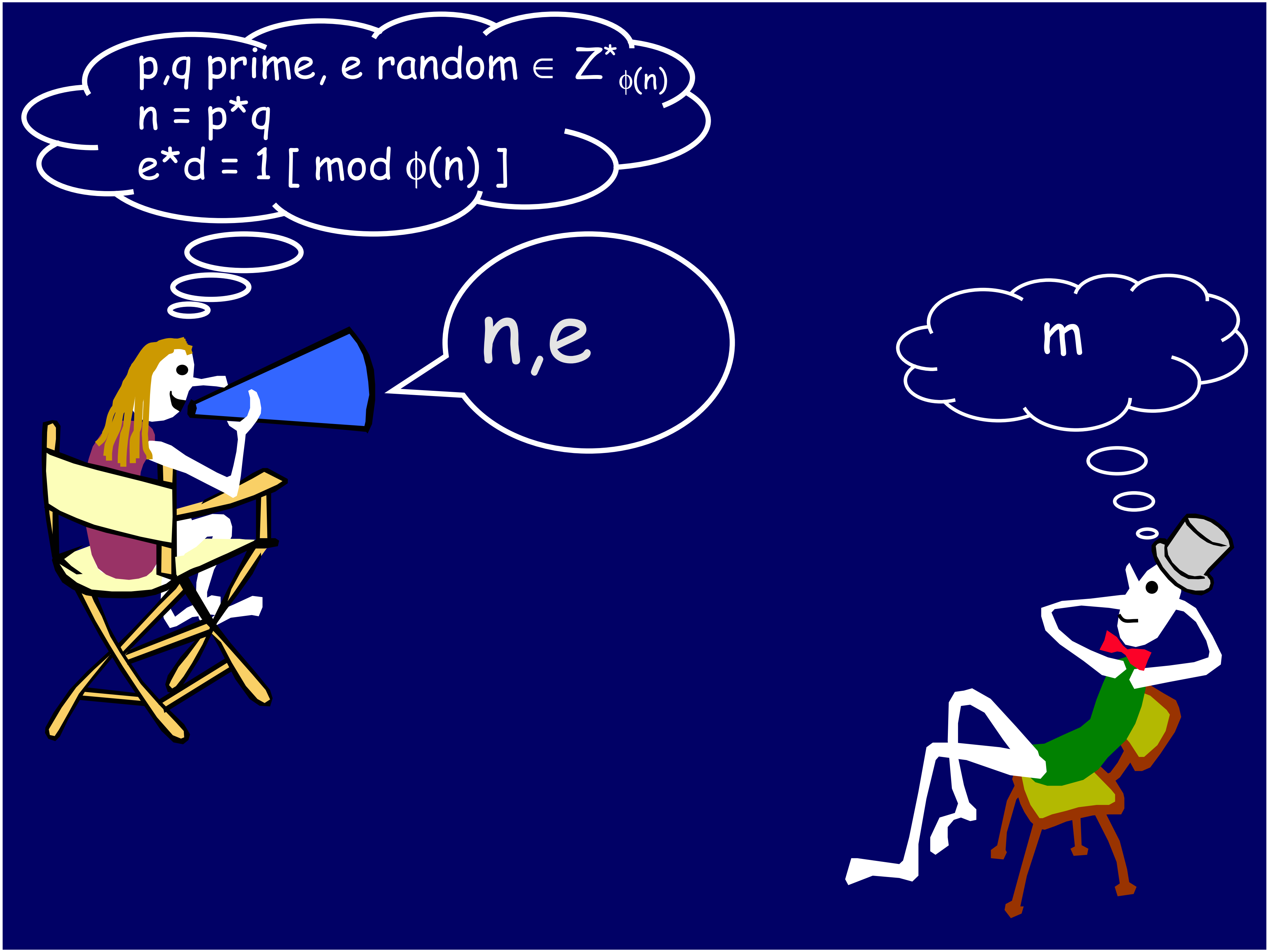
"Publish": e

Compute d = inverse of e in $Z^*_{\phi(n)}$

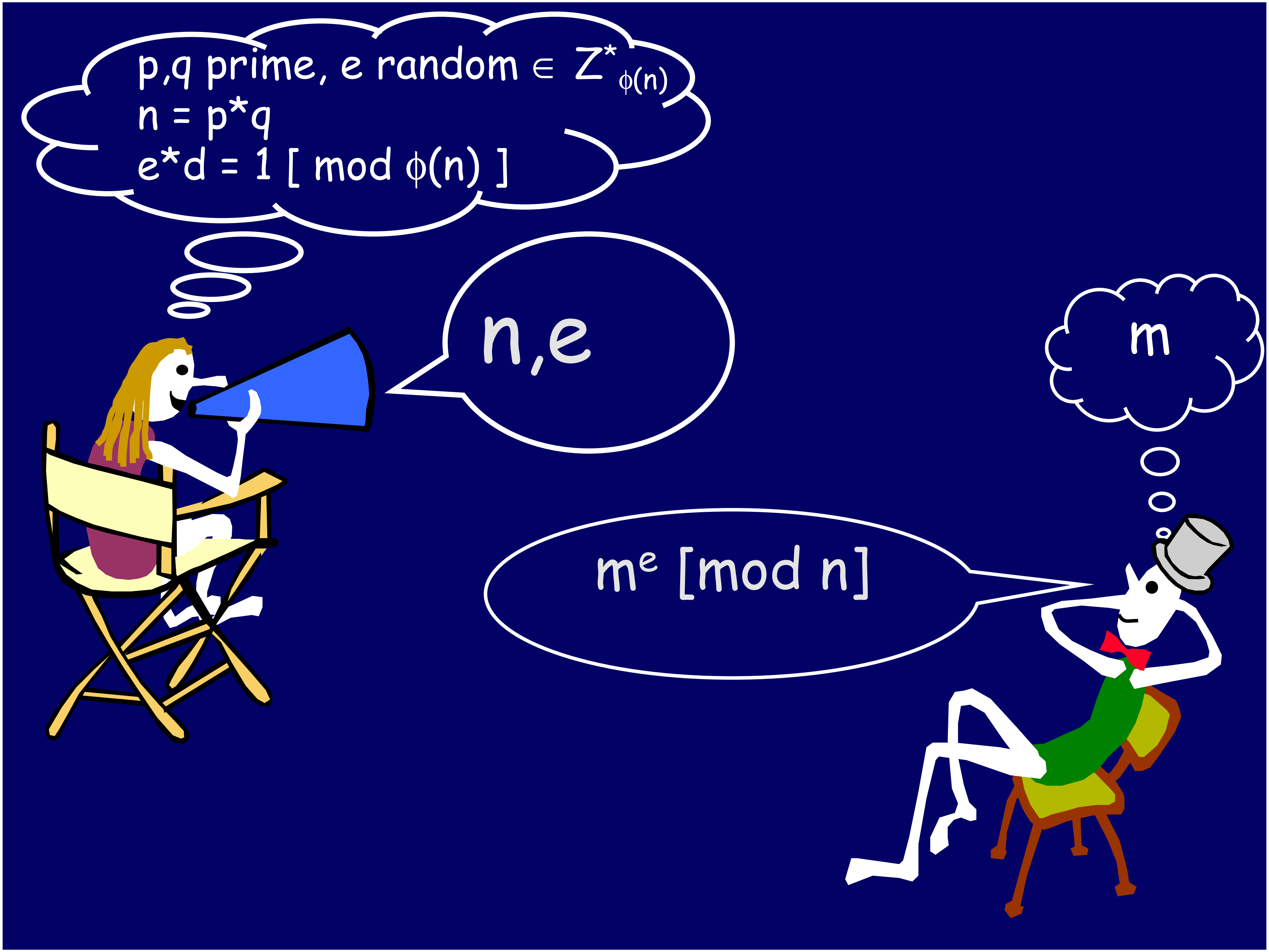
Hence, $e*d = 1$ [mod $\phi(n)$]

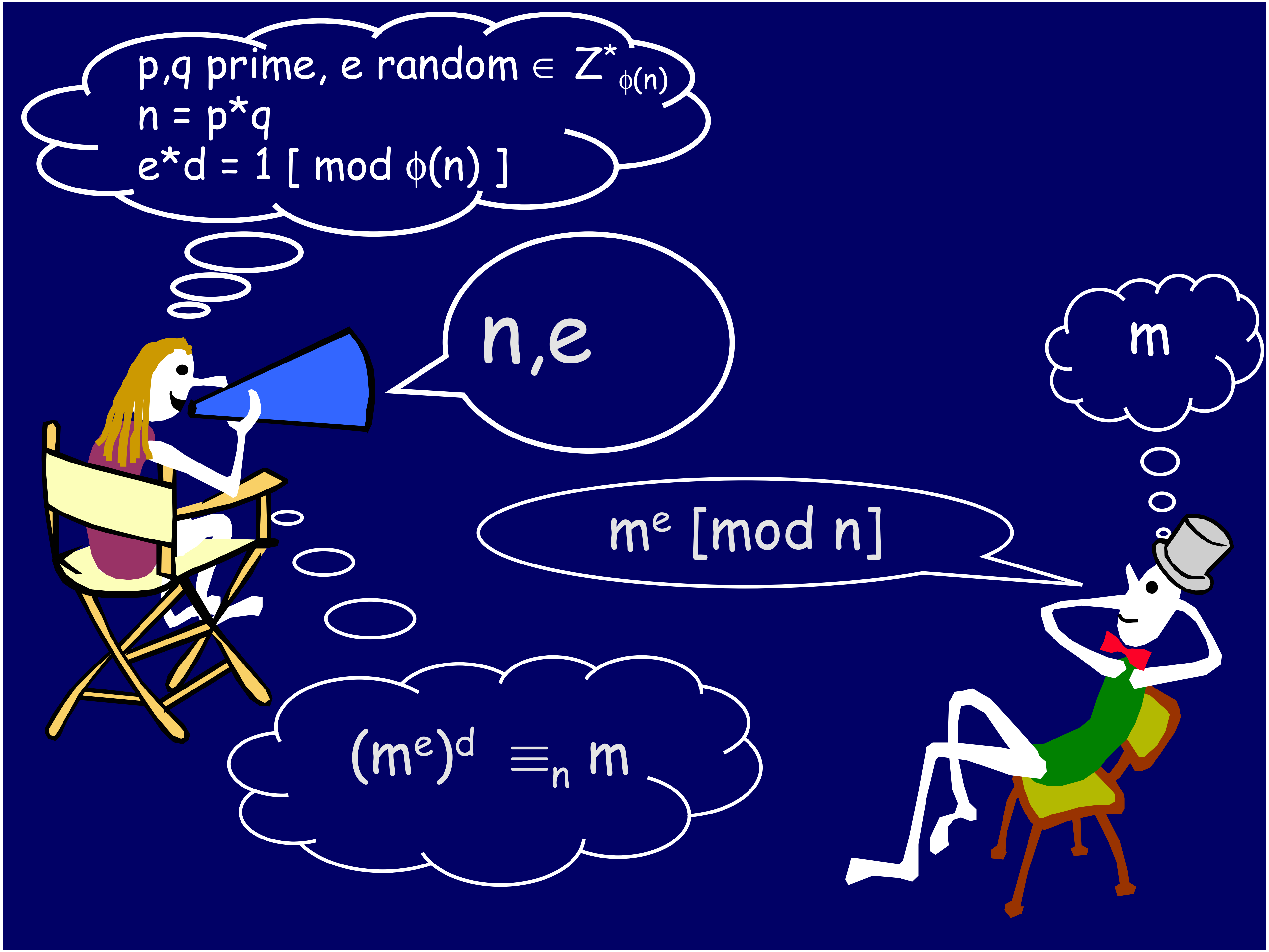
"Private Key": d


p,q random primes, e random $\in Z^*_{\phi(n)}$
n = p*q
e*d = 1 [mod $\phi(n)$]
n,e is my public key. Use it to send a message to me.



p,q prime, e random $\in Z^*_{\phi(n)}$
n = p*q
e*d = 1 [mod ϕ(n)]
n,e
m


p,q prime, e random $\in Z^*_{\phi(n)}$
$n = p*q$
$e*d = 1$ [mod $\phi(n)$]
n,e
m
m^e [mod n]



p,q prime, e random $\in Z^*_{\phi(n)}$
$n = p*q$
$e*d = 1$ [mod $\phi(n)$]
n,e
m
m^e [mod n]
$(m^e)^d \equiv_n m$