Great Theoretical Ideas In Computer Science

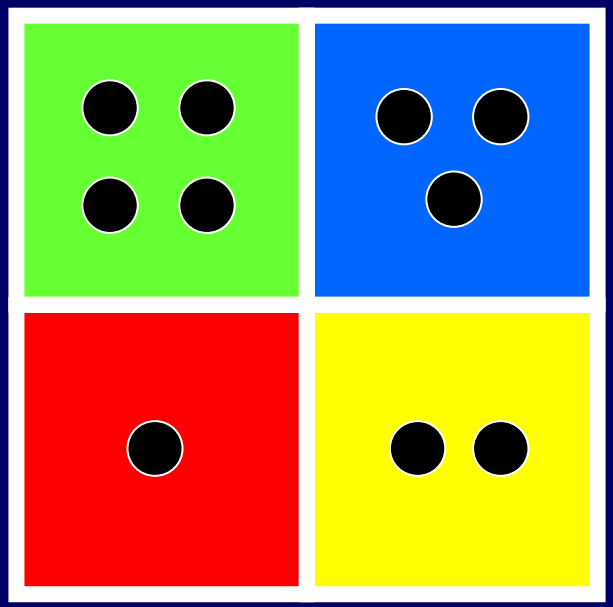
Anupam Gupta

CS 15-251 Fall 2006

Lecture 15 Oct 17, 2006

Carnegie Mellon University

Algebraic Structures: Groups, Rings, and Fields



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.

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

Quick raising to power.

$\langle Z_n, +_n \rangle$

1. Closed
2. Associative
3. 0 is identity
4. Additive Inverses
   Fast + and -
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

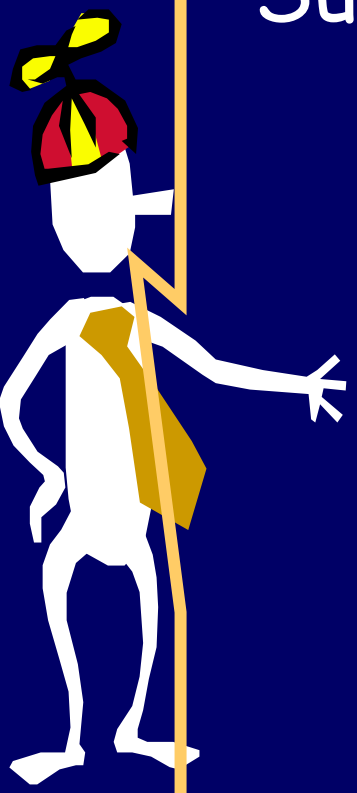
Fundamental lemma of powers.

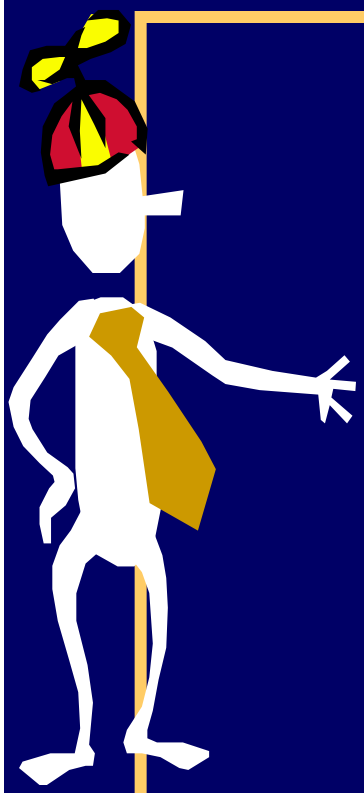
Suppose $x \in Z_n^*$, and a,b,n are naturals.

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

Equivalently,

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





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 large primes: p,q
"Publish": n = p*q

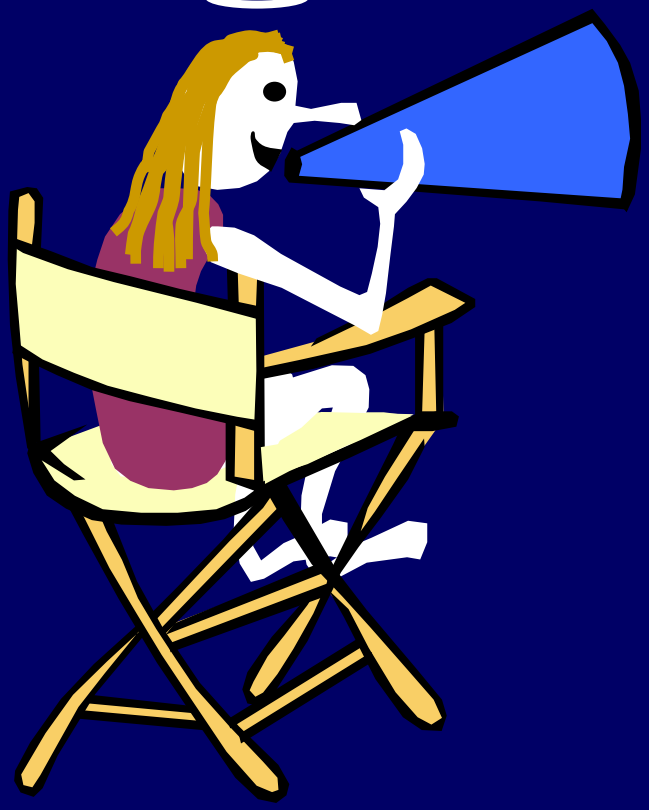
$\phi(n) = \phi(p)\,\phi(q) = (p-1)*(q-1)$
Pick random $e \in Z^*_{\phi(n)}$
"Publish": e

Compute d = inverse of e in $Z^*_{\phi(n)}$
Hence, $e*d = 1 \ [\text{ mod } \phi(n)\ ]$

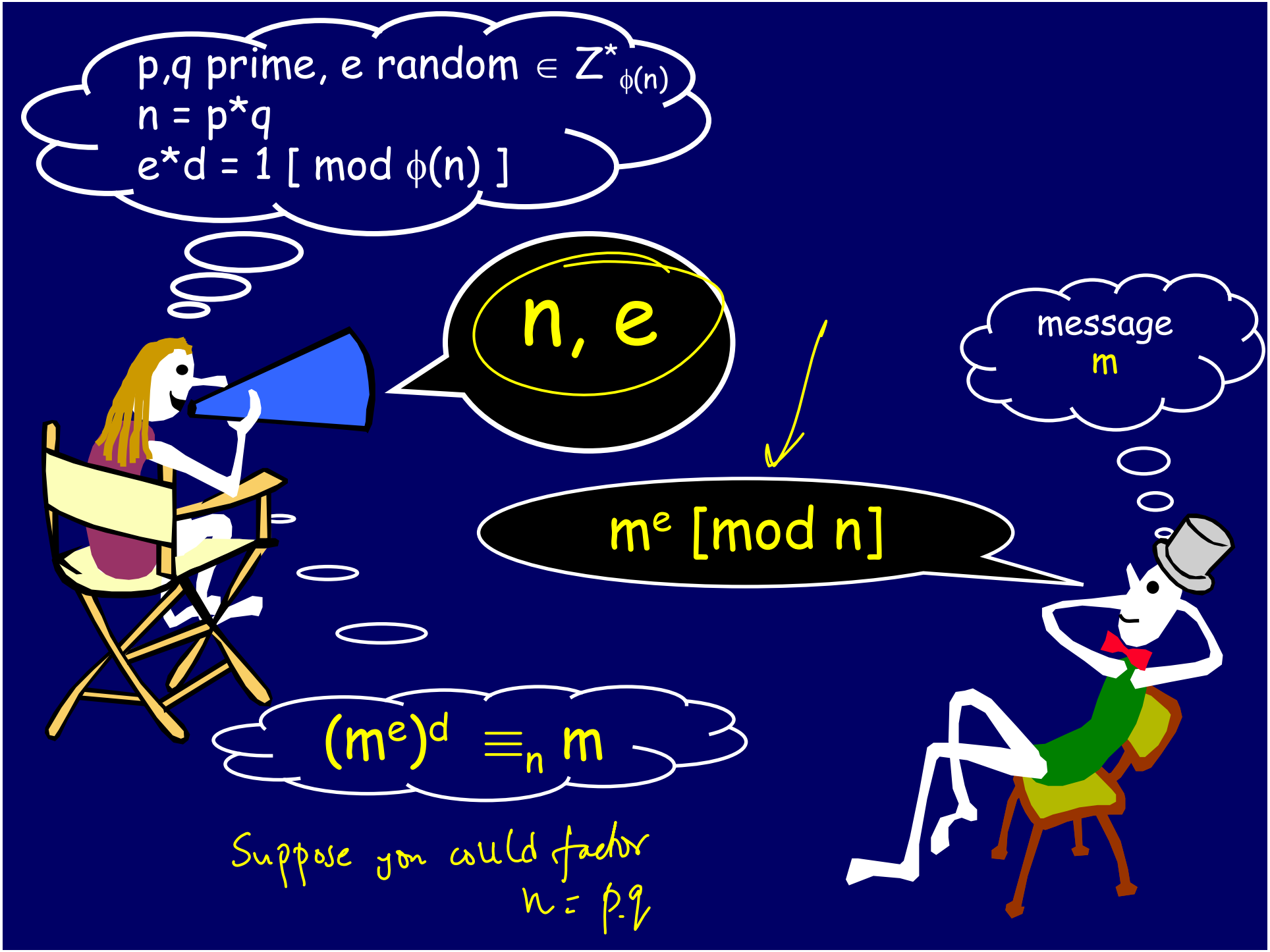
"Private Key": d

$$x^{ed} \pmod n$$
$$= x^{(ed \bmod \phi(n))} \pmod n$$
$$= x \pmod n$$

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



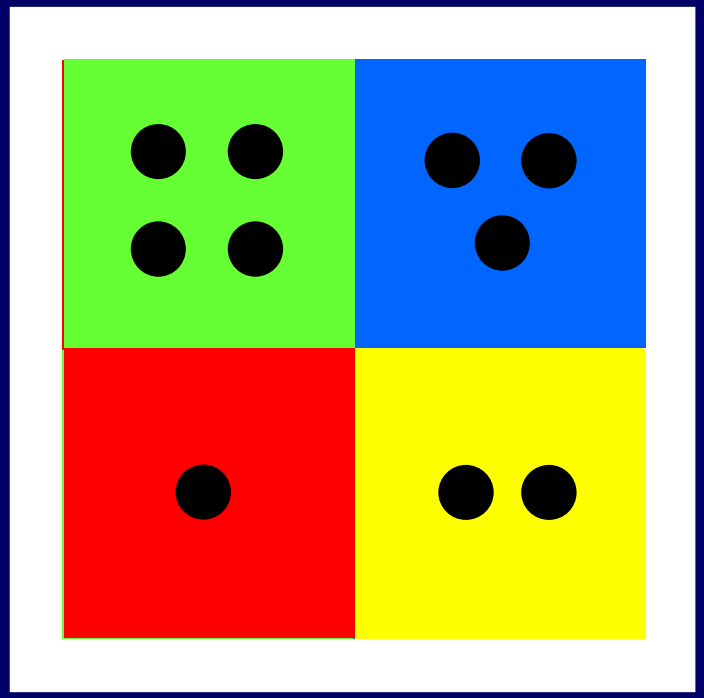
n,e is my public key. Use it to send me a message.


p,q prime, e random ∈ $Z^*_{\phi(n)}$
n = p*q
e*d = 1 [mod ϕ(n)]
n, e
message
m
m^e [mod n]
$(m^e)^d \equiv_n m$
Suppose you could factor
n = p·q

An even simpler system

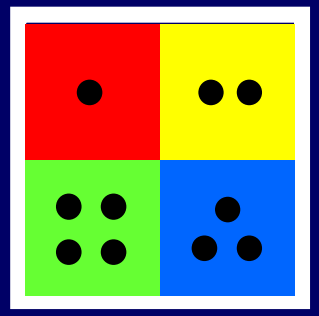
Today we are going to study the abstract properties of binary operations

Rotating a Square in Space

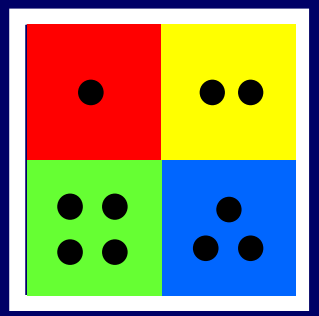


Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame

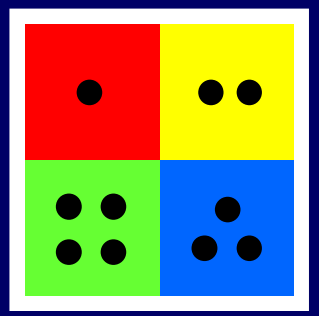
In how many different ways can we put the square back on the frame?



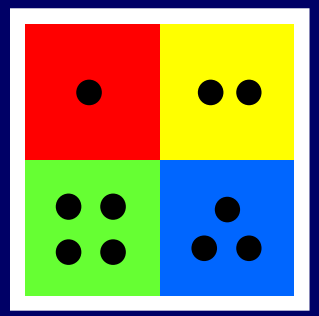
R_{90}



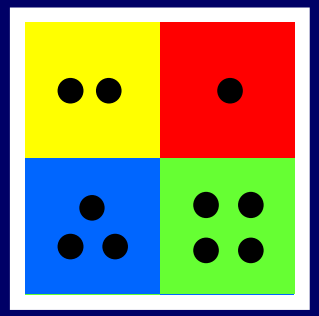
R_{180}



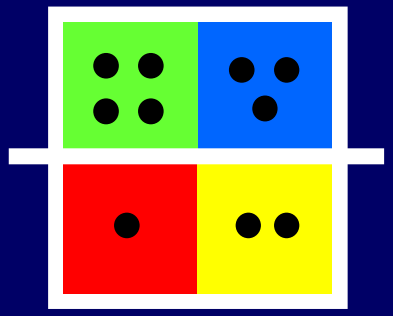
R_{270}



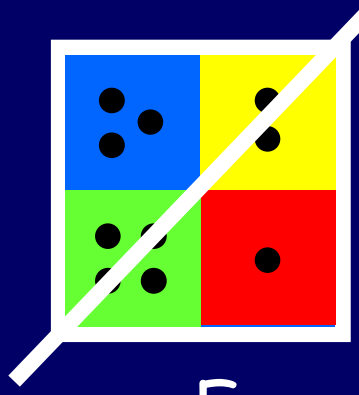
R_0



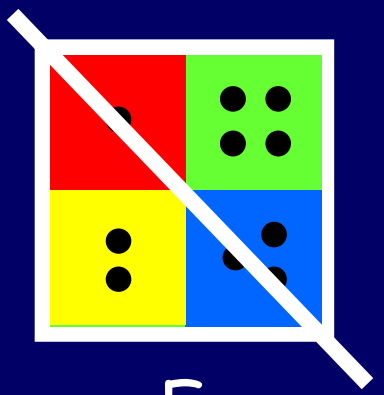
$F_|$



F_-

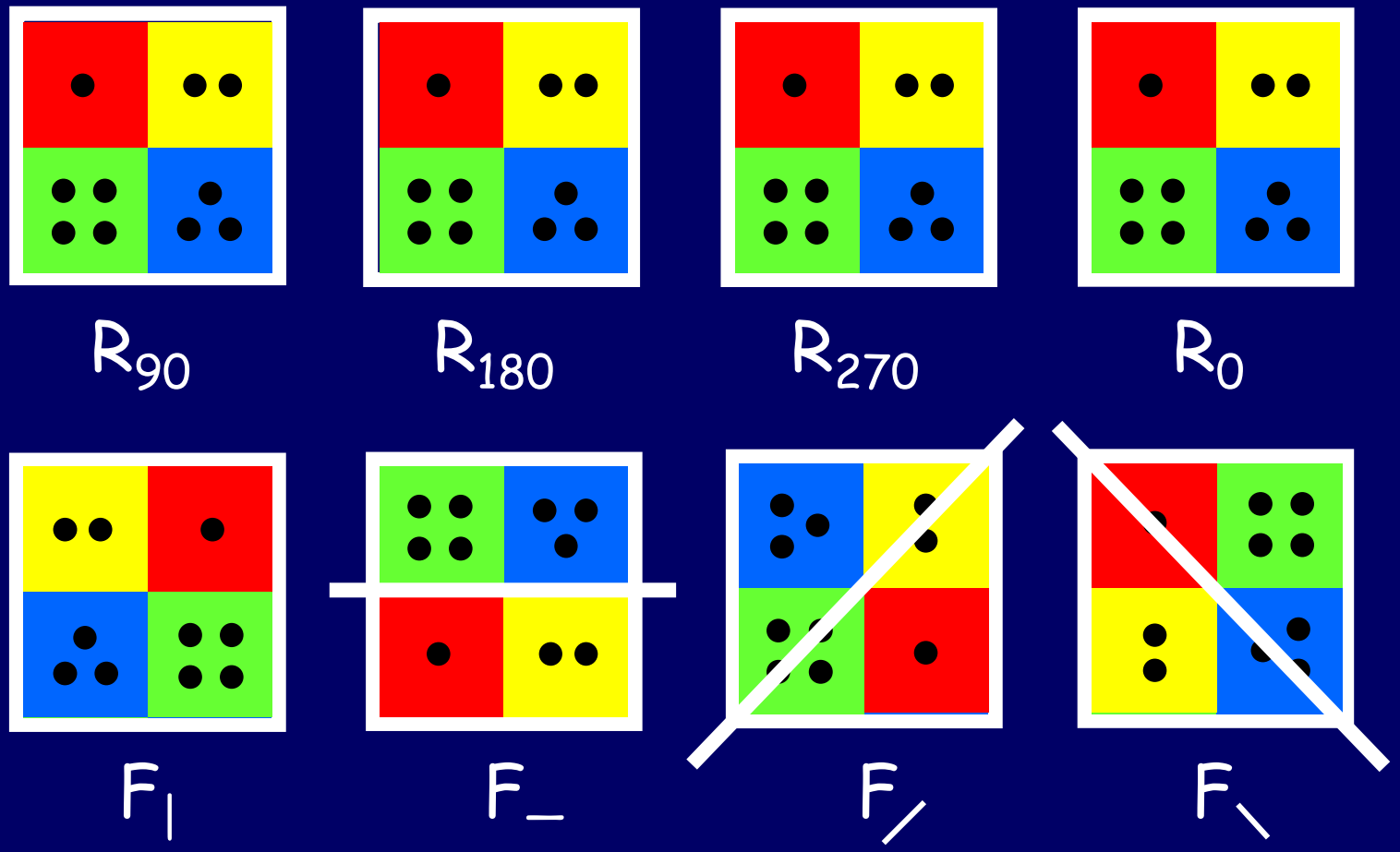


$F_/$



$F_\backslash$

We will now study these 8 motions, called symmetries of the square



Symmetries of the Square

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_|, F_-, F_/, F_\backslash \}$

Composition

Define the operation "•" to mean "first do one symmetry, and then do the next"

For example,

$R_{90} \bullet R_{180}$ means "first rotate 90° clockwise and then 180°"

$= R_{270}$

$F_{|} \bullet R_{90}$ means "first flip horizontally and then rotate 90°"

$= F_{/}$

Question: if $a,b \in Y_{SQ}$, does $a \bullet b \in Y_{SQ}$? Yes!

	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_\backslash$	$F_/$	$F_|$	F_-
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_-	$F_|$	$F_\backslash$	$F_/$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_/$	$F_\backslash$	F_-	$F_|$
$F_|$	$F_|$	$F_/$	F_-	$F_\backslash$	R_0	R_{180}	R_{90}	R_{270}
F_-	F_-	$F_\backslash$	$F_|$	$F_/$	R_{180}	R_0	R_{270}	R_{90}
$F_/$	$F_/$	F_-	$F_\backslash$	$F_|$	R_{270}	R_{90}	R_0	R_{180}
$F_\backslash$	$F_\backslash$	$F_|$	$F_/$	F_-	R_{90}	R_{270}	R_{180}	R_0

Some Formalism

If S is a set, $S \times S$ is:
the set of all (ordered) pairs of elements of S

$S \times S = \{ (a,b) \mid a \in S \text{ and } b \in S \}$

If S has n elements, how many elements does $S \times S$ have? n^2

Formally, $\bullet$ is a function from $Y_{SQ} \times Y_{SQ}$ to Y_{SQ}

$$\bullet : Y_{SQ} \times Y_{SQ} \rightarrow Y_{SQ}$$

As shorthand, we write $\bullet(a,b)$ as "$a \bullet b$"

Binary Operations

"$\bullet$" is called a binary operation on Y_{SQ}

Definition: A binary operation on a set S is a function $\blacklozenge : S \times S \to S$

Example:

The function f: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$f(x,y) = xy + y$$

is a binary operation on $\mathbb{N}$

Associativity

A binary operation ♦ on a set S is associative if:

for all $a,b,c \in S$, $(a \diamond b) \diamond c = a \diamond (b \diamond c)$

Examples:

Is f: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by f(x,y) = xy + y associative?

(ab + b)c + c = a(bc + c) + (bc + c)? NO!

Is the operation • on the set of symmetries of the square associative? YES!

Commutativity

A binary operation $\blacklozenge$ on a set S is commutative if

For all $a,b \in S$, $\quad a \blacklozenge b = b \blacklozenge a$

Is the operation $\bullet$ on the set of symmetries of the square commutative? NO!

check!

$$R_{90} \bullet F_{|} \neq F_{|} \bullet R_{90}$$

Identities

R_0 is like a null motion

Is this true: $\forall a \in Y_{SQ}$, $a \bullet R_0 = R_0 \bullet a = a$? YES!

R_0 is called the identity of $\bullet$ on Y_{SQ}

In general, for any binary operation $\blacklozenge$ on a set S, an element $e \in S$ such that for all $a \in S$,

$$e \blacklozenge a = a \blacklozenge e = a$$

is called an identity of $\blacklozenge$ on S

Inverses

Definition: The inverse of an element $a \in Y_{SQ}$ is an element b such that:

$$a \bullet b = b \bullet a = R_0$$

Examples:

R_{90} inverse: R_{270}

R_{180} inverse: R_{180}

F_I inverse: F_I

Every element in Y_{SQ} has a unique inverse

	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_\backslash$	$F_/$	$F_|$	F_-
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_-	$F_|$	$F_\backslash$	$F_/$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_/$	$F_\backslash$	F_-	$F_|$
$F_|$	$F_|$	$F_/$	F_-	$F_\backslash$	R_0	R_{180}	R_{90}	R_{270}
F_-	F_-	$F_\backslash$	$F_|$	$F_/$	R_{180}	R_0	R_{270}	R_{90}
$F_/$	$F_/$	F_-	$F_\backslash$	$F_|$	R_{270}	R_{90}	R_0	R_{180}
$F_\backslash$	$F_\backslash$	$F_|$	$F_/$	F_-	R_{90}	R_{270}	R_{180}	R_0

Groups

A group G is a pair $(S, \blacklozenge)$, where S is a set and $\blacklozenge$ is a binary operation on S such that:

1. $\blacklozenge$ is associative $\quad \forall a,b,c \in S \; (a \blacklozenge b) \blacklozenge c = a \blacklozenge (b \blacklozenge c)$
2. (Identity) There exists an element $e \in S$ such that:
   $e \blacklozenge a = a \blacklozenge e = a$, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \blacklozenge b = b \blacklozenge a = e$ (b is the inverse of a under $\blacklozenge$)

If $\blacklozenge$ is commutative, then ~~G~~ is called a commutative group (or Abelian group)

Examples

Is $(\mathbb{N},+)$ a group?

Is + associative on $\mathbb{N}$? YES!

Is there an identity? YES: 0

Does every element have an inverse? NO!

$\nexists\, a \in \mathbb{N}$ s.t. $a + (5) = 0$

$(\mathbb{N},+)$ is NOT a group

Examples

Is $(Z,+)$ a group?

Is + associative on Z? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$(Z,+)$ is a group

Examples

Is $(Y_{SQ}, \bullet)$ a group?

Is $\bullet$ associative on Y_{SQ}? YES!

Is there an identity? YES: R_0

Does every element have an inverse? YES!

$(Y_{SQ}, \bullet)$ is a group

Examples

Is $(Z_n, +)$ a group?

Is + associative on Z_n? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$a \in \mathbb{Z}_n \quad = n-a \quad -a \in \mathbb{Z}_n$

$a + (-a) = 0.$

$(Z_n, +)$ is a group

Examples

Is $(Z_n^*, *)$ a group?

Is * associative on Z_n^*? YES!

Is there an identity? YES: 1 (multiplicative identity)

Does every element have an inverse? YES!

$a \in \mathbb{Z}_n^*$ does there exist $b \in \mathbb{Z}_n^*$ s.t. $a * b = 1 \pmod n$?

$(Z_n^*, *)$ is a group

Identity Is Unique

Theorem: *A group has at most one identity element*

Proof:

Suppose e and f are both identities of $G=(S,\blacklozenge)$

Then $f = e \blacklozenge f = e$

Inverses Are Unique

Theorem: Every element in a group has a unique inverse

Proof:

Suppose b and c are both inverses of a

Then $b = b \blacklozenge e = b \blacklozenge (a \blacklozenge c) = (b \blacklozenge a) \blacklozenge c = c$

A group $G=(S,\blacklozenge)$ is finite if S is a finite set

useful notation.

Define $|G| = |S|$ to be the order of the group (i.e. the number of elements in the group)

What is the group with the least number of elements? $G = (\{e\},\blacklozenge)$ where $e \blacklozenge e = e$

How many groups of order 2 are there?

	e	f
e	e	f
f	f	e

$(\mathbb{Z}_3, +)$

Generators

A set $T \subseteq S$ is said to generate the group $G = (S, \blacklozenge)$ if every element of S can be expressed as a finite product of elements in T

Question: Does $\{R_{90}\}$ generate Y_{SQ}? NO!

Question: Does $\{S_1, R_{90}\}$ generate Y_{SQ}? YES!

set of generators for $(\mathbb{Z}, +)$ $= \{0, 1, -1\}$ or $\{-1, 1\}$

A single element $g \in S$ is called a generator of $G=(S, \blacklozenge)$ if $\{g\}$ generates G

Does Y_{SQ} have a generator? NO!

Generators For $(Z_n, +_n)$

Any $a \in Z_n$ such that GCD(a,n) = 1 generates Z_n

Claim: If GCD(a,n) =1, then the numbers
a, 2a, …, (n-1)a, na are all distinct modulo n

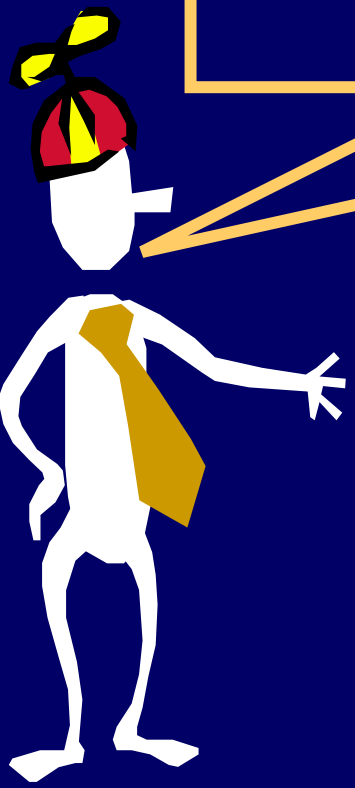
Proof (by contradiction):

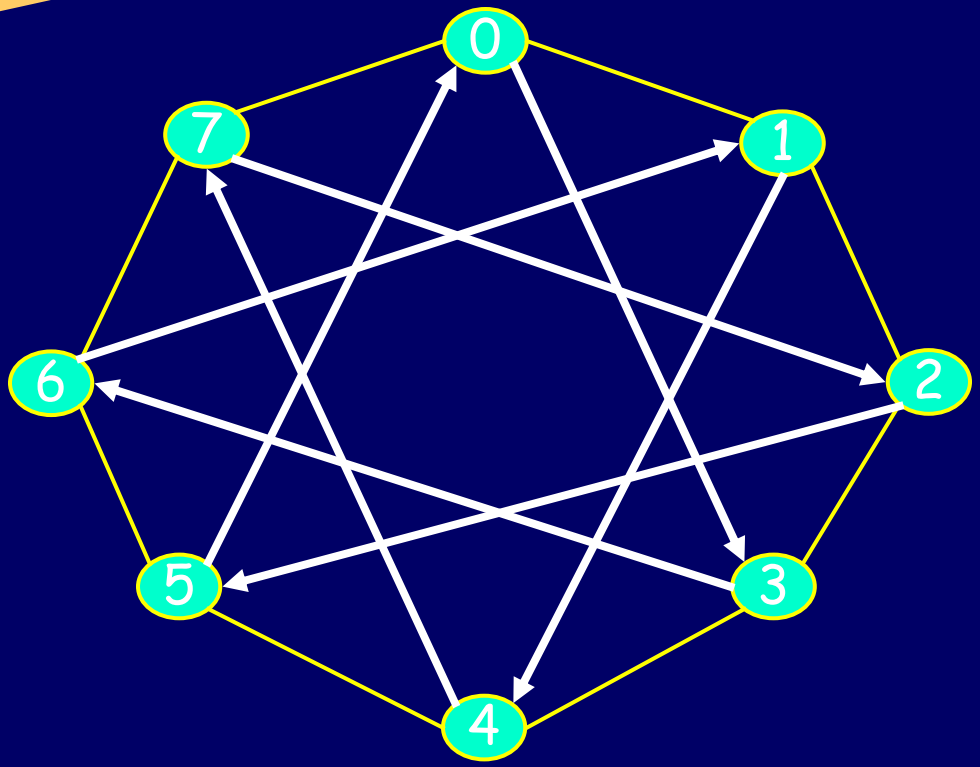
Suppose $xa = ya \pmod n$ for $x,y \in \{1,\ldots,n\}$ and $x \neq y$

Then $n \mid a(x-y)$

Since GCD(a,n) = 1, then $n \mid (x-y)$, which cannot happen

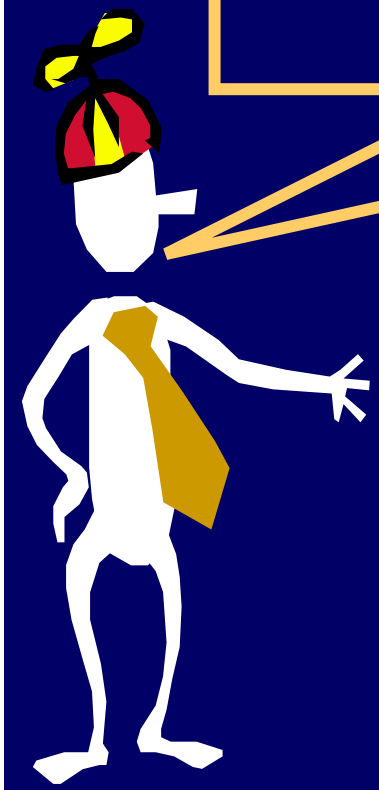
There are exactly 8 distinct multiples of 3 modulo 8.

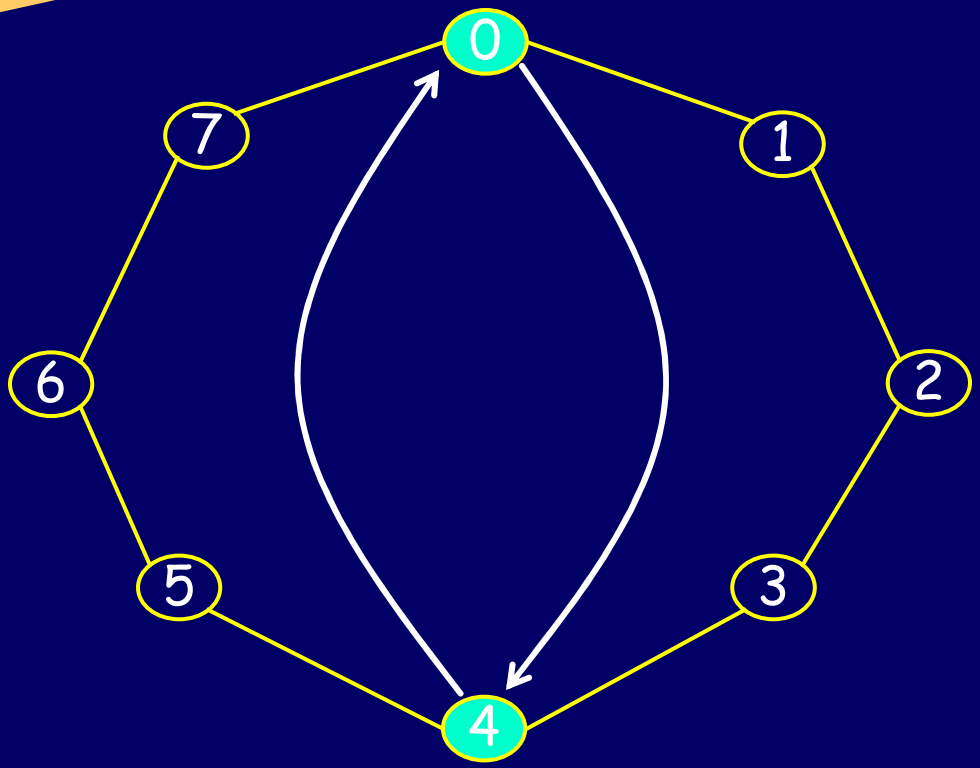




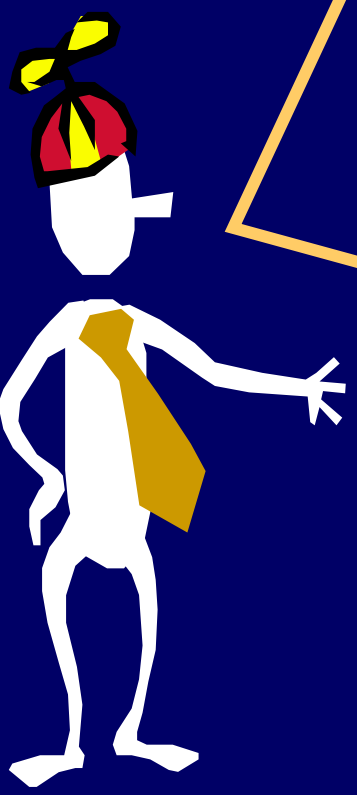
hit all numbers $\Leftrightarrow$ 3 is a generator for Z_8

There are exactly 2 distinct multiples of 4 modulo 8





4 does not generate Z_8



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

and hence

elements c with GCD(c,n) = 1
generate Z_n

Order of an element

If $G = (S, \blacklozenge)$, we use a^n denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{n \text{ times}}$

Definition: The **order** of an element a of G is the smallest positive integer n such that $a^n = e$

$n > 0$

Lemma: a is a generator of G if order(a) = |G|

If $G = (S, \blacklozenge)$, we use a^n denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{n \text{ times}}$

Definition: The order of an element a of G is the smallest positive integer n such that $a^n = e$

What is the order of F_I in Y_{SQ}? 2

What is the order of R_{90} in Y_{SQ}? 4

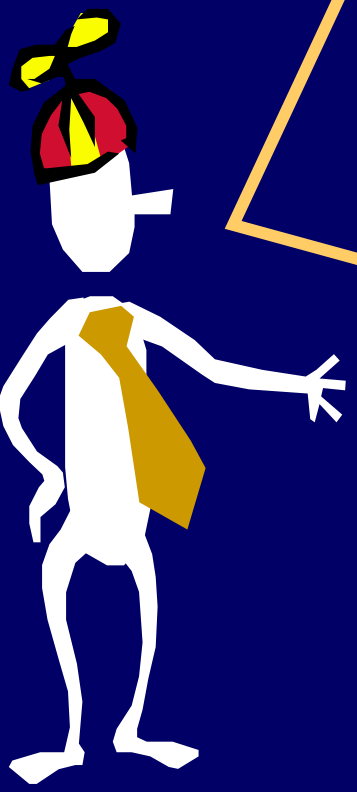
The order of an element can be infinite!
Example: The order of 1 in the group (Z,+) is infinite

Orders

What if G is a finite group:
is the order of any element of G finite?

Yes: consider $a, a^2, a^3, a^4, a^5, \ldots$
Since G is finite, at some point $a^j = a^k$ for some $j < k$.
Hence a^{k-j} = identity.

using pigeonhole!



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

and hence

$$order_{(Z_n,+)}(c) = n/GCD(c,n)$$

order(3) in $\mathbb{Z}_8$ was 8

3, 6, 1, 4, 7, 2, 5, 0

order(4) in $\mathbb{Z}_8$ = 2.

4, 0,

What about (Z_n^*, *) ?

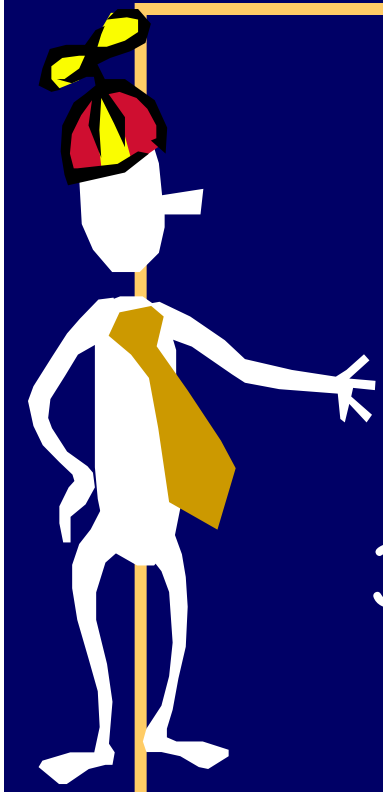
What is order of the group Z_n^*?

$|Z_n^*| = \varphi(n)$

Does Z_n^* have generators? ⟸

does $\mathbb{Z}_n^*$ have an element a with order $(a) = \varphi(n)$?

What are the orders of elements in Z_n^*?



$Z_7^* = \{1,2,3,4,5,6\}$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 1$

order(2) in $(\mathbb{Z}_7^*, *)$ is 3.

$3^0 = 1;\ 3^1 = 3;\ 3^2 = 2;\ 3^3 = 6;\ 3^4 = 4;$
$3^5 = 5;\ 3^6 = 1$

2 generates {1, 2, 4} Order 3

3 generates {1,2,3,4,5,6} Order 6

3 is a generator, but 2 is not.

of $(\mathbb{Z}_7^*, *)$

Theorem (Non-trivial)

Thm: There are $\varphi(n-1)$ generators of the group $(Z_n^*, *)$

E.g.,

for Z_7^*, $\varphi(7-1) = \varphi(2*3) = 2$.

Generators: 3,5

You can check that:

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

Orders: 1, 3, 6, 3, 6, 2

Orders

Theorem:

Let x be an element of G.
The order of x divides the order of G.

$$\text{order}(x) \mid |G|$$

proof coming soon...

Subgroups

Given a group $G = (S, \blacklozenge)$, a subset $S' \subseteq S$ forms a subgroup if $H = (S', \blacklozenge)$ satisfies the group properties.

That is,

- S' is closed under the group operation $\blacklozenge$
- The identity element of G is also in S'.
- The inverse of every element in S' is also in S'.

Y_{SQ} subgroup $Y_R = \{R_0, R_{90}, R_{180}, R_{270}\}$

Examples

$Y_{rot} = \{ R_0, R_{90}, R_{180}, R_{270} \}$

is a subgroup of

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_{|}, F_{-}, F_{/}, F_{\backslash} \}$

Quick check:

Closure?

Identity?

Inverses?

Examples

$Z_{8,even} = \{0, 2, 4, 6\}$

with the + operation is a subgroup of

$Z_8 = \{0,1,2,3,4,5,6,7\}$

Quick check:

- Closure?
- Identity?
- Inverses?

Lagrange's Theorem

Theorem: if H is a subgroup of G, then $|H|$ divides $|G|$.

Fact: The set generated by any element $x \in G$ is a subgroup of G.

$S' = \{x, x^2, x^3, \ldots\}$ subgroup of S

$|S'| = \text{order}(x) \mid |S|$

Corollary: the order of any element $x \in G$ divides $|G|$.

Proof of Lagrange's Theorem

Lord Of The Rings

We can define more than one operation on a set

For example, in Z_n we can do addition and multiplication modulo n

A ring is a set together with two operations (usually called + and *)

Definition:

A ring R is a set together with two binary operations + and *, satisfying the following properties:

1. (R,+) is a commutative group

2. * is associative

3. The distributive laws hold in R:

$$(a + b) * c = (a * c) + (b * c)$$

$$a * (b + c) = (a * b) + (a * c)$$

Examples

Do the integers $\mathbb{Z}$ form a ring?

($\mathbb{Z}$, +) is a commutative group.

* is associative

+ distributes over *…

Fields

Definition:

A field F is a set together with two binary operations + and *, satisfying the following properties:

1. (F,+) is a commutative group
2. (F-{0},*) is a commutative group
3. The distributive law holds in F:

$$(a + b) * c = (a * c) + (b * c)$$

Examples

Do the integers $\mathbb{Z}$ form a field?

$(\mathbb{Z}, +)$ is a commutative group.

but $(\mathbb{Z}\backslash\{0\}, *)$ do not form a group!

there are no multiplicative inverses…

Examples

Z_p (for prime p) is a field.

$(Z_p, +)$ is a commutative group.

$(Z_p^* = Z_p \setminus \{0\}, *)$ is a commutative group.

The distributive law holds.

Examples

The real numbers $\mathbb{R}$ form a field.

$(\mathbb{R}, +)$ is a commutative group.

$(\mathbb{R}\backslash\{0\}, *)$ is a commutative group.

The distributive law holds.

CRYPTOGRAPHY based on the presumed computational difficulty of a number theoretic problem.

Let p be prime. g be a generator for $(Z_p^*, *)$

$DH_{p.g}(x) = g^x \bmod p$ is fast to compute.

$DISCRETE\text{-}LOG_{p,g}(r) = x$ means that $g^x = r \bmod p$.

No one knows a fast algorithm given a random r to compute x.

Diffie and Hellman [1976]
"New Directions In Cryptography."

Let p be prime. g be a generator mod p.

Alice: Picks random $x \in Z_{p-1}$
Publishes $g^x \bmod p$

Bob: Picks random $y \in Z_{p-1}$
Publishes $g^y \bmod p$

does not know x & y

Eve sees both published strings.

Can she figure out $g^{xy} \bmod p$?

Both parties can compute (mod p)
$(g^x)^y = (g^y)^x = g^{xy \bmod p-1}$

Diffie Hellman has an *amazing* feature.

Two people who have never met and have no prior shared secrets can use the system.

Without this property, commerce on the net would be impossible.

Typical use: Agree on a random string r.
Use r as your secret-key in a more conventional private-key crypto system

In The End…

Why should I care about any of this?

Groups, Rings and Fields are examples of the principle of abstraction: the particulars of the objects are abstracted into a few simple properties

All the results carry over to any group

Ideas central to crypto and other areas!

Study Bee

Symmetries of the Square

Compositions

Groups

Binary Operation

Identity and Inverses

Basic Facts: Inverses Are Unique

Generators

Rings and Fields

Definition