CMSC/Math 456: Cryptography (Fall 2022)

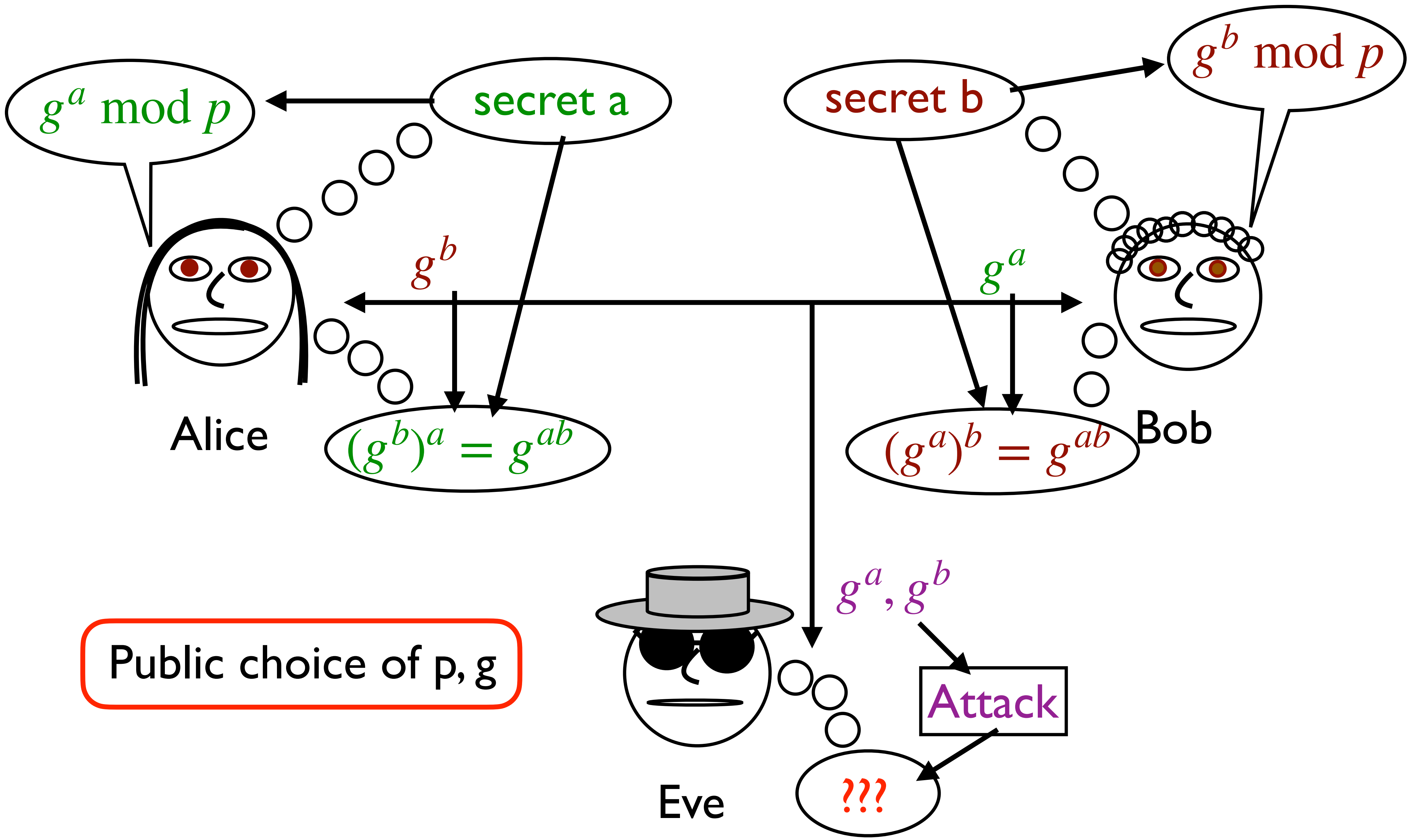
Lecture 10

Daniel Gottesman

Administrative

Problem set #3 should have been turned in. Grades for problem set #2 are out. Problem set #4 is available now, due next Thursday, Oct. 6.

Diffie-Hellman Key Exchange



Public choice of p, g

Diffie-Hellman Security Idea

In Diffie-Hellman, Alice and Bob must perform modular exponentiation: Alice announces $A = g^a \bmod p$ and Bob announces $B = g^b \bmod p$ for secret a and b chosen by Alice and Bob respectively and not shared with each other or Eve. Then they do another pair of modular exponentiations B^a and A^b to calculate the key.

- Alice and Bob must compute modular exponentials, which can be done in polynomial time in the *length* of p, g.

Eve can break Diffie-Hellman if she can calculate the discrete log for (g,p): That is, if given y, she can find x such that $g^x = y \bmod p$.

- So, for security, we need that calculating the discrete log is hard.

We are studying modular arithmetic to understand the difficulty of discrete log.

Modular Arithmetic

Modular addition, subtraction, and multiplication work essentially the same way as the same operations on integers, and can be done efficiently using standard algorithms.

Modular division mod N can only be done if we are dividing by b such that $\gcd(b, N) = 1$. In that case, b^{-1} can be efficiently calculated using Euclid's algorithm.

Modular exponentiation can be done efficiently through repeated squaring. An element g has an order ord(g) such that $g^{\mathrm{ord}(g)} = 1 \bmod N$ but $g^r \neq 1 \bmod N$ for $r < \mathrm{ord}(g)$.

In fact, modular exponentials repeat after ord(g). That is,

$$g^a = g^b \bmod p \text{ iff } a = b \bmod \mathrm{ord}(g)$$

What values of ord(g) are possible?

$\mathbb{Z}_N^*$

Recall that we are focusing on g such that $\gcd(b, N) = 1$ so that division is well-defined and some power of g gives 1.

Definition: Let $\mathbb{Z}_N^*$ be the set of $g \in \{0, \ldots, N-1\}$ such that $\gcd(b, N) = 1$.

Proposition: If $\gcd(g, N) = 1$ and $\gcd(h, N) = 1$, then $\gcd(gh, N) = 1$ as well. I.e., $\mathbb{Z}_N^*$ is closed under multiplication.

Proof:

Recall that x^{-1} is well-defined mod N iff $\gcd(x, N) = 1$. But $(gh)^{-1} = h^{-1}g^{-1}$:

$$(h^{-1}g^{-1})(gh) = h^{-1} \cdot 1 \cdot h \bmod N = 1 \bmod N$$

This means that gh has an inverse and therefore $\gcd(gh, N) = 1$.

Groups

Definition: A group (G, *) is a set G of elements along with a binary operation $* : G \times G \rightarrow G$ with the following properties:

1. Closure: $g * h \in G$ when $g, h \in G$.
2. Associativity: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
3. Identity: $\exists e \in G$ such that $\forall g \in G, e * g = g * e = g$.
4. Inverses: $\forall g \in G, \exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A group which also satisfies

5. Commutativity: $\forall g, h \in G, g * h = h * g$

is called an abelian group.

Usually we just refer to G as the group. If we need to specify the group operation, we say "G under [operation]." Usually instead of *, the group operation is just written + or $\cdot$ like addition or multiplication even if it is not those.

This class is being recorded

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ under multiplication? Vote

Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

$\mathbb{Z}_N$ under addition? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote. — Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote — Yes.

Integers $\mathbb{Z}$ under multiplication? Vote — No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote — No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ under multiplication? Vote — Yes.

$\mathbb{R}^*$ under exponentiation? Vote — No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

$\mathbb{Z}_N$ under addition? Vote — Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.	Bad question. Which group operation?
Integers $\mathbb{Z}$ under addition? Vote	Yes.
Integers $\mathbb{Z}$ under multiplication? Vote	No. No inverses.
Reals $\mathbb{R}$ under multiplication? Vote	No. 0 still has no inverse.
$\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ under multiplication? Vote	Yes.
$\mathbb{R}^*$ under exponentiation? Vote	No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)
$\mathbb{Z}_N$ under addition? Vote	Yes.
$\mathbb{Z}_N^*$ under multiplication? Vote	

This class is being recorded

Group Examples

For each of the following, vote on whether it is a group: yes/no/ bad question.

Integers $\mathbb{Z}$? Vote.	Bad question. Which group operation?
Integers $\mathbb{Z}$ under addition? Vote	Yes.
Integers $\mathbb{Z}$ under multiplication? Vote	No. No inverses.
Reals $\mathbb{R}$ under multiplication? Vote	No. 0 still has no inverse.
$\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ under multiplication? Vote	Yes.
$\mathbb{R}^*$ under exponentiation? Vote	No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)
$\mathbb{Z}_N$ under addition? Vote	Yes.
$\mathbb{Z}_N^*$ under multiplication? Vote	Yes.

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

Definition: The order of a finite group G is written $|G|$ and is equal to the number of elements in G.

Examples:

The set of even integers forms a subgroup of $\mathbb{Z}$ under addition.

$\mathbb{Z}_5$ is not a subgroup of $\mathbb{Z}$ under addition: The addition operation is different, since in $\mathbb{Z}_5$, $3 + 3 = 1$, whereas in $\mathbb{Z}$, $3 + 3 = 6$.

$|\mathbb{Z}_5| = 5$ and $|\mathbb{Z}_5^*| = 4$.

Lagrange's Theorem

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: We will write the group operation as multiplication.

Let $gH = \{gh | h \in H\}$. Since $gh = gh'$ iff $h = h'$ (multiply by g^{-1}), $|gH| = |H|$.

Lagrange's Theorem

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: We will write the group operation as multiplication.

Let $gH = \{gh \mid h \in H\}$. Since $gh = gh'$ iff $h = h'$ (multiply by g^{-1}), $|gH| = |H|$.

Claim: Now, if $g' = gk$ for $k \in H$, then $gH = g'H$:

$g'H = \{gkh \mid h \in H\}$ but $kh \in H$ (by closure of H). kh can take on any value $h' \in H$, when $h = k^{-1}h'$. (k^{-1} is in H by the inverses property of H and the product is in H by closure again.)

Lagrange's Theorem

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: We will write the group operation as multiplication.

Let $gH = \{gh | h \in H\}$. Since $gh = gh'$ iff $h = h'$ (multiply by g^{-1}), $|gH| = |H|$.

Claim: Now, if $g' = gk$ for $k \in H$, then $gH = g'H$:

$g'H = \{gkh | h \in H\}$ but $kh \in H$ (by closure of H). kh can take on any value $h' \in H$, when $h = k^{-1}h'$. (k^{-1} is in H by the inverses property of H and the product is in H by closure again.)

Claim: If $g' \neq gk$ for all $k \in H$, that means that $gH \cap g'H = \varnothing$:

If $gh = g'h' \in gH \cap g'H$, then $g' = ghh'^{-1}$, but $hh'^{-1} \in H$ by the closure and inverses properties of H, and this contradicts $g' \neq gk$ for $k \in H$.

This class is being recorded

Lagrange's Theorem

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: We will write the group operation as multiplication.

Let $gH = \{gh | h \in H\}$. Since $gh = gh'$ iff $h = h'$ (multiply by g^{-1}), $|gH| = |H|$.

Claim: Now, if $g' = gk$ for $k \in H$, then $gH = g'H$:

$g'H = \{gkh | h \in H\}$ but $kh \in H$ (by closure of H). kh can take on any value $h' \in H$, when $h = k^{-1}h'$. (k^{-1} is in H by the inverses property of H and the product is in H by closure again.)

Claim: If $g' \neq gk$ for all $k \in H$, that means that $gH \cap g'H = \varnothing$:

If $gh = g'h' \in gH \cap g'H$, then $g' = ghh'^{-1}$, but $hh'^{-1} \in H$ by the closure and inverses properties of H, and this contradicts $g' \neq gk$ for $k \in H$.

The distinct gH partition G, so $|gH| = |H|$ divides $|G|$.

This class is being recorded

Generators and Cyclic Groups

Definition: Let G be a group. A set $S \subseteq G$ is a generating set for G if any element of G can be written as a finite product (under the group operation) of elements of S or inverses of elements of S, with repeats allowed. Note: S is a subset of G. It need not be a subgroup of G.

A group is cyclic if it has a generating set with just a single element.

Examples:

$\{1\}$ is a generating set for $\mathbb{Z}$, so $\mathbb{Z}$ is cyclic. (Under addition, since otherwise $\mathbb{Z}$ is not a group.)

$\{2,3\}$ is also a generating set for $\mathbb{Z}$, as is any pair $\{a, b\}$ with gcd(a,b) = 1. Proof: Euclid's algorithm.

$\{1\}$ is a generating set for $\mathbb{Z}_5$ (under addition), as is $\{a\}$ for any $a \neq 0$.

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now we can finally return to the question of what are the possible orders of a number under modular exponentiation.

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

(Why is it a subgroup? $g^a g^b = g^{a+b}$, so it is closed, and $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$, so $\langle g \rangle$ has inverses since $(g^a)^{-1} = (g^{-1})^a$.)

By Lagrange's Theorem, $\mathrm{ord}(g) = |\langle g \rangle|$ divides $|\mathbb{Z}_N^*|$. This tells us the possible values of the order of g: the factors of $|\mathbb{Z}_N^*|$.

When N is prime, then everything smaller than N is relatively prime to it, so $|\mathbb{Z}_N^*| = N - 1$.

What is $|\mathbb{Z}_N^*|$ when N is not prime?

This class is being recorded