

## Lecture 7. Outline.

1. Isoperimetric inequality for hypercube.
2. Modular Arithmetic.  
Clock Math!!!
3. Inverses for Modular Arithmetic: Greatest Common Divisor.  
Division!!!
4. Euclid's GCD Algorithm.  
A little tricky here!

# Isoperimetry.

For 3-space:

The sphere minimizes surface area to volume.

Surface Area:  $4\pi r^2$ , Volume:  $\frac{4}{3}\pi r^3$ .

Ratio:  $1/3r = \Theta(V^{-1/3})$ .

Graphical Analog: Cut into two pieces and find ratio of edges/vertices on small side.

Tree:  $\Theta(1/|V|)$ .

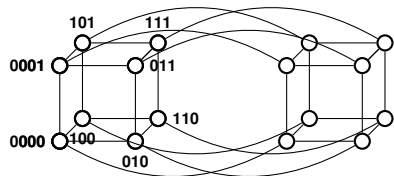
Hypercube:  $\Theta(1)$ .

Surface Area is roughly at least the volume!

## Recursive Definition.

A 0-dimensional hypercube is a node labelled with the empty string of bits.

An  $n$ -dimensional hypercube consists of a 0-subcube (1-subcube) which is a  $n - 1$ -dimensional hypercube with nodes labelled  $0x$  ( $1x$ ) with the additional edges  $(0x, 1x)$ .



(A),(C),(D)

- (A) Lower left forward node name is 0000
- (B) Lower left back node name is 0001
- (C) Upper right forward node is 1011
- (D) Upper right back node name is 1111

# Hypercube: Can't cut me!

**Thm:** Any subset  $S$  of the hypercube where  $|S| \leq |V|/2$  has  $\geq |S|$  edges connecting it to  $V - S$ ;  $|E \cap S \times (V - S)| \geq |S|$

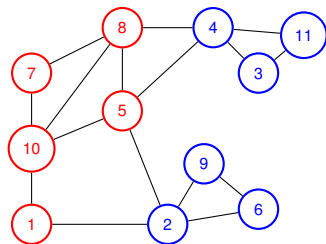
Terminology:

$(S, V - S)$  is cut.

$(E \cap S \times (V - S))$  - cut edges.

Restatement: for any cut in the hypercube, the number of cut edges is at least the size of the small side.

## Cuts in graphs.



$S$  is red,  $V - S$  is blue.

What is size of cut?

Number of edges between red and blue. 4.

Hypercube: any cut that cuts off  $x$  nodes has  $\geq x$  edges.

# Proof of Large Cuts.

**Thm:** For any cut  $(S, V - S)$  in the hypercube, the number of cut edges is at least the size of the small side.

**Proof:**

Base Case:  $n = 1$   $V = \{0, 1\}$ .

$S = \{0\}$  has one edge leaving.  $|S| = \phi$  has 0.

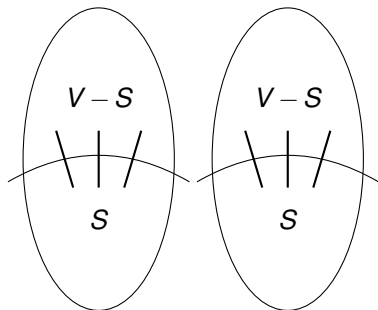
# Induction Step Idea

**Thm:** For any cut  $(S, V - S)$  in the hypercube, the number of cut edges is at least the size of the small side.

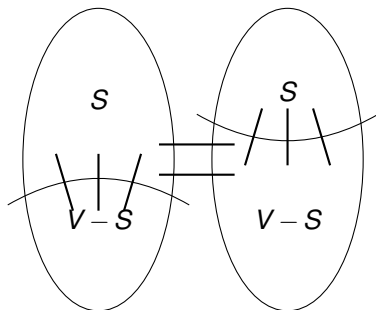
Use recursive definition into two subcubes.

Two cubes connected by edges.

Case 1: Count edges inside subcube inductively.



Case 2: Count inside and across.



# Induction Step

**Thm:** For any cut  $(S, V - S)$  in the hypercube, the number of cut edges is at least the size of the small side,  $|S|$ .

**Proof: Induction Step.**

Recursive definition:

$H_0 = (V_0, E_0), H_1 = (V_1, E_1)$ , edges  $E_x$  that connect them.

$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$

$S = S_0 \cup S_1$  where  $S_0$  in first, and  $S_1$  in other.

**Case 1:**  $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$

Both  $S_0$  and  $S_1$  are small sides. So by induction.

Edges cut in  $H_0 \geq |S_0|$ .

Edges cut in  $H_1 \geq |S_1|$ .

Total cut edges  $\geq |S_0| + |S_1| = |S|$ . □



## Induction Step. Case 2.

**Thm:** For any cut  $(S, V - S)$  in the hypercube, the number of cut edges is at least the size of the small side,  $|S|$ .

**Proof: Induction Step. Case 2.**

$$|S_0| \geq |V_0|/2.$$

Recall Case 1:  $|S_0|, |S_1| \leq |V|/2$

$$|S_1| \leq |V_1|/2 \text{ since } |S| \leq |V|/2.$$

$\implies \geq |S_1|$  edges cut in  $E_1$ .

$$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$$

$\implies \geq |V_0| - |S_0|$  edges cut in  $E_0$ .

Edges in  $E_x$  connect corresponding nodes.

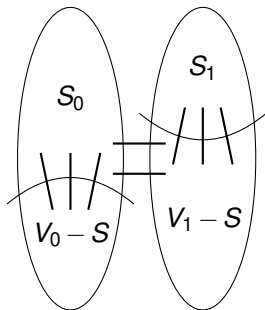
$\implies = |S_0| - |S_1|$  edges cut in  $E_x$ .

Total edges cut:

$$\geq |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$$

$$|V_0| = |V|/2 \geq |S|.$$

Also, case 3 where  $|S_1| \geq |V|/2$  is symmetric. □



# Hypercube proof: poll

## **Hypercube has large cuts proof uses these ideas:**

- (A) If cuts are same size on two sides it works by induction.
  - (B) Uses the fact that it is planar.
  - (C) Recursive definition of hypercube.
  - (D) If different size, can count edges between to subcubes.
  - (E) Applies Euler's formula.
- (A),(D), and (E).

# Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 sets to 1 set on boolean functions on  $\{0, 1\}^n$ .

Central area of study in computer science!

Yes/No Computer Programs  $\equiv$  Boolean function on  $\{0, 1\}^n$

Central object of study.

# Modular Arithmetic.

Applications: cryptography, error correction.

## Key ideas for modular arithmetic.

Theorem: If  $d|x$  and  $d|y$ , then  $d|(y - x)$ .

Proof:

$$x = ad, y = bd,$$

$$(x - y) = (ad - bd) = d(a - b) \implies d|(x - y).$$

□

Theorem: Every number  $n \geq 2$  can be represented as a product of primes.

Proof: Either prime, or  $n = a \times b$ , and use strong induction.  
(Uniqueness? Later.)

□

## What did we use in our proofs of key ideas?

- (A) Distributive Property of multiplication over addition.
- (B) Euler's formula.
- (C) The definition of a prime number.
- (D) Euclid's Lemma.
- (A) and (C)

Next Up.

Modular Arithmetic.

# Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.

Clock time equivalent up to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.

$$101 = 12 \times 8 + 5.$$

5 is the same as 101 for a 12 hour clock system.

Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in  $\{12, 1, \dots, 11\}$

(Almost remainder, except for 12 and 0 are equivalent.)



## Day of the week.

This is Thursday is September 16, 2021.

What day is it a year from then? on September 16, 2022?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 4.

5 days from then. day 9 or day 2 or Tuesday.

25 days from then. day 29 or day 1.  $29 = (7)4 + 1$

two days are equivalent up to addition/subtraction of multiple of 7.

11 days from then is day 1 which is Monday!

What day is it a year from then?

Next year is not a leap year. So 365 days from then.

Day  $4+365$  or day 369.

Smallest representation:

subtract 7 until smaller than 7.

divide and get remainder.

$369/7$  leaves quotient of 52 and remainder 5.  $369 = 7(52) + 5$

or September 16, 2022 is a Friday.

## Years and years...

80 years? 20 leap years.  $366 \times 20$  days

60 regular years.  $365 \times 60$  days

Today is day 4.

It is day  $4 + 366 \times 20 + 365 \times 60$ . Equivalent to?

Hmm.

What is remainder of 366 when dividing by 7?  $52 \times 7 + 2$ .

What is remainder of 365 when dividing by 7? 1

Today is day 4.

Get Day:  $4 + 2 \times 20 + 1 \times 60 = 104$

Remainder when dividing by 7?  $104 = 14 \times 7 + 6$ .

Or February 11, 2101 is Saturday!

Further Simplify Calculation:

20 has remainder 6 when divided by 7.

60 has remainder 4 when divided by 7.

Get Day:  $2 + 2 \times 6 + 1 \times 4 = 18$ .

Or Day 6. September 16, 2101 is Saturday.

“Reduce” at any time in calculation!

## Modular Arithmetic: refresher.

$x$  is congruent to  $y$  modulo  $m$  or “ $x \equiv y \pmod{m}$ ”

if and only if  $(x - y)$  is divisible by  $m$ .

...or  $x$  and  $y$  have the same remainder w.r.t.  $m$ .

...or  $x = y + km$  for some integer  $k$ .

Mod 7 equivalence classes:

$\{\dots, -7, 0, 7, 14, \dots\}$   $\{\dots, -6, 1, 8, 15, \dots\}$  ...

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent  $x$  and  $y$ .

or “ $a \equiv c \pmod{m}$  and  $b \equiv d \pmod{m}$ ”

$\implies a + b \equiv c + d \pmod{m}$  and  $a \cdot b \equiv c \cdot d \pmod{m}$ ”

**Proof:** If  $a \equiv c \pmod{m}$ , then  $a = c + km$  for some integer  $k$ .

If  $b \equiv d \pmod{m}$ , then  $b = d + jm$  for some integer  $j$ .

Therefore,  $a + b = c + d + (k + j)m$  and since  $k + j$  is integer.

$\implies a + b \equiv c + d \pmod{m}$ . □

Can calculate with representative in  $\{0, \dots, m - 1\}$ .

# Notation

$x \pmod{m}$  or  $\text{mod}(x, m)$

- remainder of  $x$  divided by  $m$  in  $\{0, \dots, m-1\}$ .

$$\text{mod}(x, m) = x - \lfloor \frac{x}{m} \rfloor m$$

$\lfloor \frac{x}{m} \rfloor$  is quotient.

$$\text{mod}(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \del{5} = 5$$

Work in this system.

$$a \equiv b \pmod{m}.$$

Says two integers  $a$  and  $b$  are equivalent modulo  $m$ .

**Modulus** is  $m$

$$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}.$$

$$6 = 3 + 3 = 3 + 10 \pmod{7}.$$

Generally, not  $6 \pmod{7} = 13 \pmod{7}$ .

But probably won't take off points, still hard for us to read.

# Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies \left(\frac{1}{2}\right) \cdot 2x = \left(\frac{1}{2}\right) \cdot 3 \implies x = \frac{3}{2}.$$

**Multiplicative inverse of  $x$  is  $y$  where  $xy = 1$ ;  
1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of  $x \bmod m$  is  $y$  with  $xy = 1 \pmod{m}$ .**

For 4 modulo 7 inverse is 2:  $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$ .

Can solve  $4x = 5 \pmod{7}$ .

$$x = 3 \pmod{7} \implies 4(3) = 12 \equiv 5 \pmod{7}.$$

For 8 modulo 12: no multiplicative inverse!

$$x = 3 \pmod{7}$$

“Common factor of 4”  
Check!  $4(3) = 12 \equiv 0 \pmod{7}$ .

$8k - 12\ell$  is a multiple of four for any  $\ell$  and  $k \implies$

$$8k \not\equiv 1 \pmod{12} \text{ for any } k.$$

# Poll

## Mark true statements.

- (A) Multiplicative inverse of 2 mod 5 is 3 mod 5.
  - (B) The multiplicative inverse of  $((n-1) \pmod n) = ((n-1) \pmod n)$ .
  - (C) Multiplicative inverse of 2 mod 5 is 0.5.
  - (D) Multiplicative inverse of  $4 = -1 \pmod 5$ .
  - (E)  $(-1) \times (-1) = 1$ . Woohoo.
  - (F) Multiplicative inverse of 4 mod 5 is 4 mod 5.
- (C) is false. 0.5 has no meaning in arithmetic modulo 5.

# Greatest Common Divisor and Inverses.

## Thm:

If greatest common divisor of  $x$  and  $m$ ,  $\gcd(x, m)$ , is 1, then  $x$  has a multiplicative inverse modulo  $m$ .

## Proof $\implies$ :

**Claim:** The set  $S = \{0x, 1x, \dots, (m-1)x\}$  contains  $y \equiv 1 \pmod{m}$  if all distinct modulo  $m$ .

Each of  $m$  numbers in  $S$  correspond to one of  $m$  equivalence classes modulo  $m$ .

$\implies$  One must correspond to 1 modulo  $m$ . **Inverse Exists!**

Proof of Claim: If not distinct, then  $\exists a, b \in \{0, \dots, m-1\}$ ,  $a \neq b$ , where  
 $(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$

Or  $(a-b)x = km$  for some integer  $k$ .

$$\gcd(x, m) = 1$$

$\implies$  Prime factorization of  $m$  and  $x$  do not contain common primes.

$\implies (a-b)$  factorization contains all primes in  $m$ 's factorization.

So  $(a-b)$  has to be multiple of  $m$ .

$\implies (a-b) \geq m$ . But  $a, b \in \{0, \dots, m-1\}$ . Contradiction.  $\square$

## Proof review. Consequence.

**Thm:** If  $\gcd(x, m) = 1$ , then  $x$  has a multiplicative inverse modulo  $m$ .

**Proof Sketch:** The set  $S = \{0x, 1x, \dots, (m-1)x\}$  contains  $y \equiv 1 \pmod{m}$  if all distinct modulo  $m$ .

...

For  $x = 4$  and  $m = 6$ . All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$   
reducing  $\pmod{6}$

$$S = \{0, 4, 2, 0, 4, 2\}$$

Not distinct. Common factor 2. Can't be 1. No inverse.

For  $x = 5$  and  $m = 6$ .

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$   
All distinct, contains 1! 5 is multiplicative inverse of 5  $\pmod{6}$ .

(Hmm. What normal number is it own multiplicative inverse?) 1 -1.

$5x = 3 \pmod{6}$  What is  $x$ ? Multiply both sides by 5.

$$x = 15 = 3 \pmod{6}$$

$4x = 3 \pmod{6}$  No solutions. Can't get an odd.

$4x = 2 \pmod{6}$  Two solutions!  $x = 2, 5 \pmod{6}$

Very different for elements with inverses.





## Proof Review 2: Bijections.

If  $\gcd(x,m) = 1$ .

Then the function  $f(a) = xa \pmod m$  is a bijection.

One to one: there is a unique pre-image.

Onto: the sizes of the domain and co-domain are the same.

$x = 3, m = 4$ .

$f(1) = 3(1) = 3 \pmod 4, f(2) = 6 = 2 \pmod 4, f(3) = 1 \pmod 4$ .

Oh yeah.  $f(0) = 0$ .

Bijection  $\equiv$  unique pre-image and same size.

All the images are distinct.  $\implies$  unique pre-image for any image.

$x = 2, m = 4$ .

$f(1) = 2, f(2) = 0, f(3) = 2$

Oh yeah.  $f(0) = 0$ .

Not a bijection.

# Poll

## Which is bijection?

(A)  $f(x) = x$  for domain and range being  $\mathbb{R}$

(B)  $f(x) = ax \pmod{n}$  for  $x \in \{0, \dots, n-1\}$  and  $\gcd(a, n) = 2$

(C)  $f(x) = ax \pmod{n}$  for  $x \in \{0, \dots, n-1\}$  and  $\gcd(a, n) = 1$

(B) is not.

# Only if

Thm: If  $\gcd(x, m) \neq 1$  then  $x$  has no multiplicative inverse modulo  $m$ .

Assume  $a$  is  $x^{-1}$ , or  $ax = 1 + km$ .

$x = nd$  and  $m = \ell d$  for  $d > 1$ .

Thus,

$$a(nd) = 1 + k\ell d \text{ or } d(na - k\ell) = 1.$$

But  $d > 1$  and  $n = (na - k\ell) \in \mathbb{Z}$ .

so  $dn \neq 1$  and  $dn = 1$ . Contradiction.



## Finding inverses.

How to find the inverse?

How to find **if**  $x$  has an inverse modulo  $m$ ?

Find  $\gcd(x, m)$ .

Greater than 1? No multiplicative inverse.

Equal to 1? Multiplicative inverse.

Algorithm: Try all numbers up to  $x$  to see if it divides both  $x$  and  $m$ .

Very slow.

# Inverses

Next up.

Euclid's Algorithm.

Runtime.

Euclid's Extended Algorithm.

# Refresh

Does 2 have an inverse mod 8? No.

Any multiple of 2 is 2 away from  $0 + 8k$  for any  $k \in \mathbb{N}$ .

Does 2 have an inverse mod 9? Yes. 5

$$2(5) = 10 = 1 \pmod{9}.$$

Does 6 have an inverse mod 9? No.

Any multiple of 6 is 3 away from  $0 + 9k$  for any  $k \in \mathbb{N}$ .

$$3 = \gcd(6, 9)!$$

$x$  has an inverse modulo  $m$  if and only if

$\gcd(x, m) > 1$ ? No.

$\gcd(x, m) = 1$ ? Yes.

Now what?:

Compute gcd!

Compute Inverse modulo  $m$ .

# Divisibility...

**Notation:**  $d|x$  means “ $d$  divides  $x$ ” or  
 $x = kd$  for some integer  $k$ .

**Fact:** If  $d|x$  and  $d|y$  then  $d|(x + y)$  and  $d|(x - y)$ .

Is it a fact? Yes? No?

**Proof:**  $d|x$  and  $d|y$  or  
 $x = \ell d$  and  $y = kd$

$$\implies x - y = kd - \ell d = (k - \ell)d \implies d|(x - y)$$



## More divisibility

**Notation:**  $d|x$  means “ $d$  divides  $x$ ” or  
 $x = kd$  for some integer  $k$ .

**Lemma 1:** If  $d|x$  and  $d|y$  then  $d|y$  and  $d| \text{ mod } (x, y)$ .

**Proof:**

$$\begin{aligned}\text{mod } (x, y) &= x - \lfloor x/y \rfloor \cdot y \\ &= x - \lfloor s \rfloor \cdot y \quad \text{for integer } s \\ &= kd - sl d \quad \text{for integers } k, \ell \text{ where } x = kd \text{ and } y = \ell d \\ &= (k - s\ell)d\end{aligned}$$

Therefore  $d| \text{ mod } (x, y)$ . And  $d|y$  since it is in condition. □

**Lemma 2:** If  $d|y$  and  $d| \text{ mod } (x, y)$  then  $d|y$  and  $d|x$ .

**Proof...:** Similar. Try this at home. □ish.

**GCD Mod Corollary:**  $\text{gcd}(x, y) = \text{gcd}(y, \text{ mod } (x, y))$ .

**Proof:**  $x$  and  $y$  have **same** set of common divisors as  $x$  and  $\text{mod } (x, y)$  by Lemma 1 and 2.

Same common divisors  $\implies$  largest is the same. □



## Euclid's algorithm.

**GCD Mod Corollary:**  $\gcd(x, y) = \gcd(y, \text{mod}(x, y))$ .

Hey, what's  $\gcd(7, 0)$ ? 7 since 7 divides 7 and 7 divides 0

What's  $\gcd(x, 0)$ ? x

```
(define (euclid x y)
  (if (= y 0)
      x
      (euclid y (mod x y)))) ***
```

**Theorem:**  $(\text{euclid } x \ y) = \gcd(x, y)$  if  $x \geq y$ .

**Proof:** Use Strong Induction.

**Base Case:**  $y = 0$ , “x divides y and x”

$\implies$  “x is common divisor and clearly largest.”

**Induction Step:**  $\text{mod}(x, y) < y \leq x$  when  $x \geq y$

call in line (\*\*\*) meets conditions plus arguments “smaller”

and by strong induction hypothesis

computes  $\gcd(y, \text{mod}(x, y))$

which is  $\gcd(x, y)$  by GCD Mod Corollary. □

## Modular Arithmetic Lecture in a minute.

Modular Arithmetic:  $x \equiv y \pmod{N}$  if  $x = y + kN$  for some integer  $k$ .

For  $a \equiv b \pmod{N}$ , and  $c \equiv d \pmod{N}$ ,  
 $ac \equiv bd \pmod{N}$  and  $a + b \equiv c + d \pmod{N}$ .

Division? Multiply by multiplicative inverse.

$a \pmod{N}$  has multiplicative inverse,  $a^{-1} \pmod{N}$ .

If and only if  $\gcd(a, N) = 1$ .

Why? If:  $f(x) = ax \pmod{N}$  is a bijection on  $\{1, \dots, N-1\}$ .

$ax - ay = 0 \pmod{N} \implies a(x - y)$  is a multiple of  $N$ .

If  $\gcd(a, N) = 1$ ,

then  $(x - y)$  must contain all primes in prime factorization of  $N$ ,  
and is therefore be bigger than  $N$ .

Only if: For  $a = xd$  and  $N = yd$ ,

any  $ma + kN = d(mx - ky)$  or is a multiple of  $d$ ,  
and is not 1.

Euclid's Alg:  $\gcd(x, y) = \gcd(y \pmod{x}, x)$

Fast cuz value drops by a factor of two every two recursive calls.

Know if there is an inverse, but how do we find it? On Tuesday!