Chapter 3
Algorithms and Complexity

Dr. Mohammed Marey

2018

What is an algorithm

A finite set (or sequence) of precise instructions

for performing a computation.

Example: Maxima finding

procedure *max* (*a1, a2, …, an*: integers)

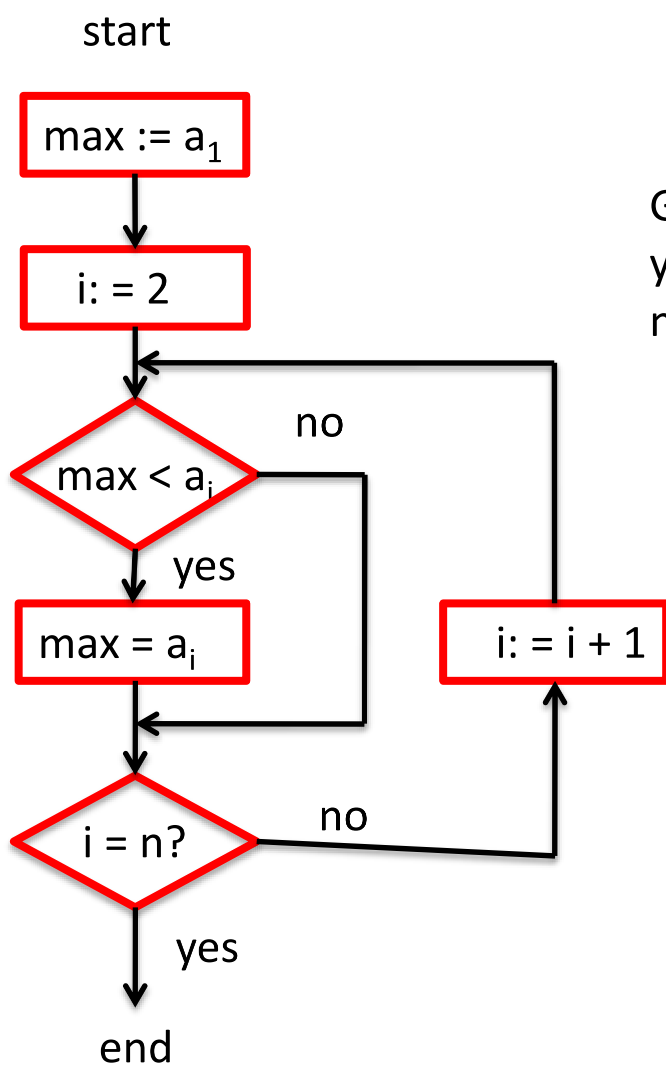
max := *a1*

for i :=*2* to *n*

    if *max* < *a1* then *max* := *ai*

return *max* {the largest element}

Flowchart for maxima finding



Given n elements, can you count the total number of operations?

Time complexity of algorithms

Measures the largest number of ***basic operations*** *required to execute an algorithm.*

Example: Maxima finding

procedure *max* (*a1, a2, …, an*: integers)

max := *a1* — *1 operation*

for i :=*2* to *n* — *n-1 times*

if *max* < *a1* then *max* := *ai* — *2 operations*

return *max* {the largest element}

The total number of operations is 2n-1

Time complexity of algorithms

Example of linear search (Search x in a list $a_1\ a_2\ a_3 \ldots a_n$*)*

k := 1 (1 operation)

while k ≤ n do

{if x = a_k then *found* else k: = k+1} (2n operations)

search failed

The maximum number of operations is 2n+1. If we are lucky, then search can end even in a single step.

Sorting algorithm

Sort a list ***$a_1\, a_2\, a_3 \ldots a_n$ in the ascending order***

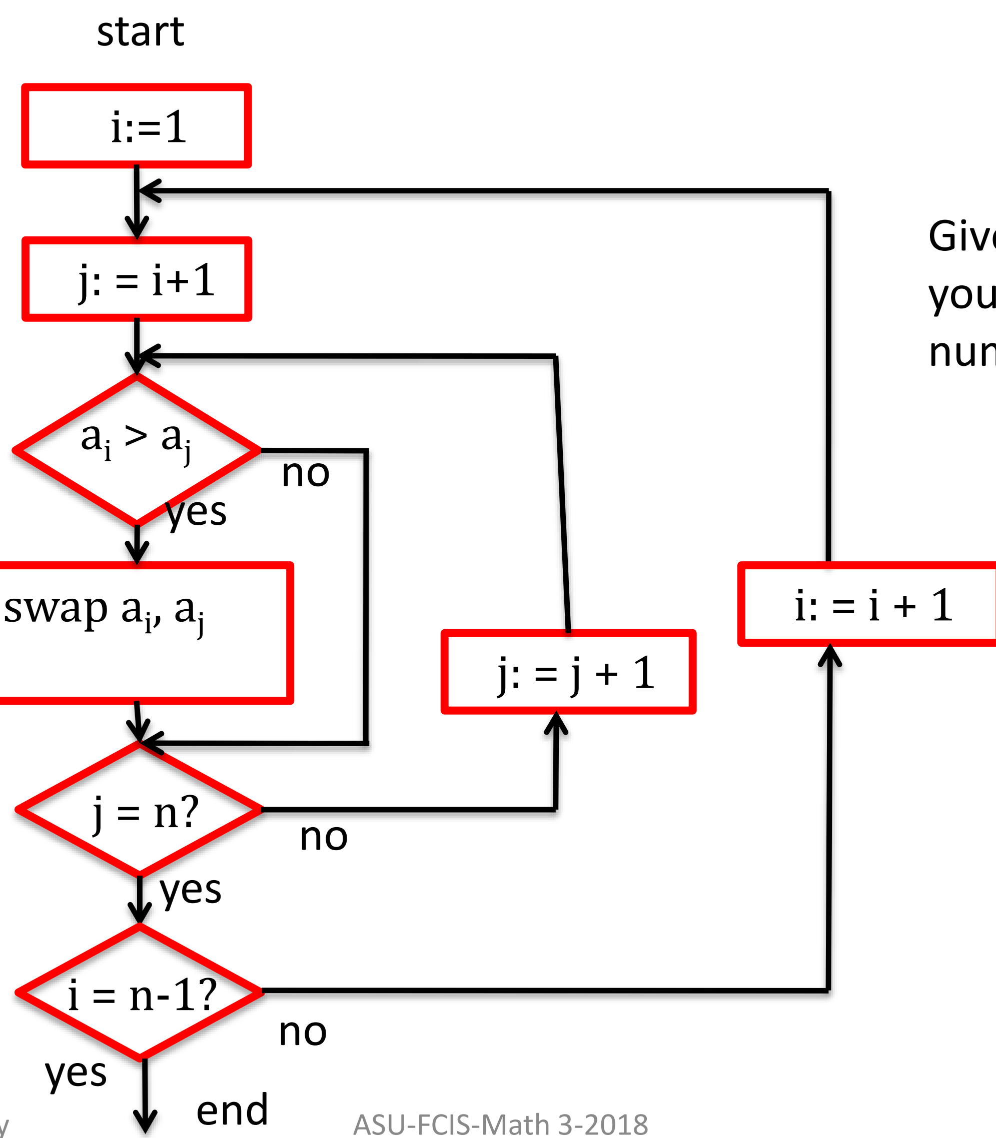
for i:= 1 to n-1

  for j:= i+1 to n

    if $a_i > a_j$ then swap $(a_i\, ,\, a_j)$

How many basic operations will you need here?

Example of a sorting algorithm



Given n elements, can you count the total number of operations?

Bubble Sort

Procedure bubblesort
{sort n integers $a_1, a_2, \ldots, a_n$ in ascending order}
    for i:= 1 to n-1
        for j:= 1 to n-i
            if $a_j > a_{j+1}$ then swap (a_j, a_{j+1})

3	2	4	1	5		n-1 operations
2	3	1	4	5	(first pass)	n-2 operations
2	1	3	4	5	(second pass)	n-3 operations
1	2	3	4	5	(third pass)	…
1	2	3	4	5	(fourth pass)	1

Bubble Sort

3	2	4	1	5		n-1 operations
2	3	1	4	5	(first pass)	n-2 operations
2	1	3	4	5	(second pass)	n-3 operations
1	2	3	4	5	(third pass)	…
1	2	3	4	5	(fourth pass)	1

The worst case time complexity is

$$(n-1) + (n-2) + (n-3) + \ldots + 2 + 1$$
$$= n(n-1)/2$$

The Big-O notation

It is a measure of the growth of functions and often used to measure the complexity of algorithms.

DEF. Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. Then f is O(g(x)) if there are constants **C** and **k**, such that

$$|f(x)| \leq C|g(x)| \qquad \text{for all } x > k$$

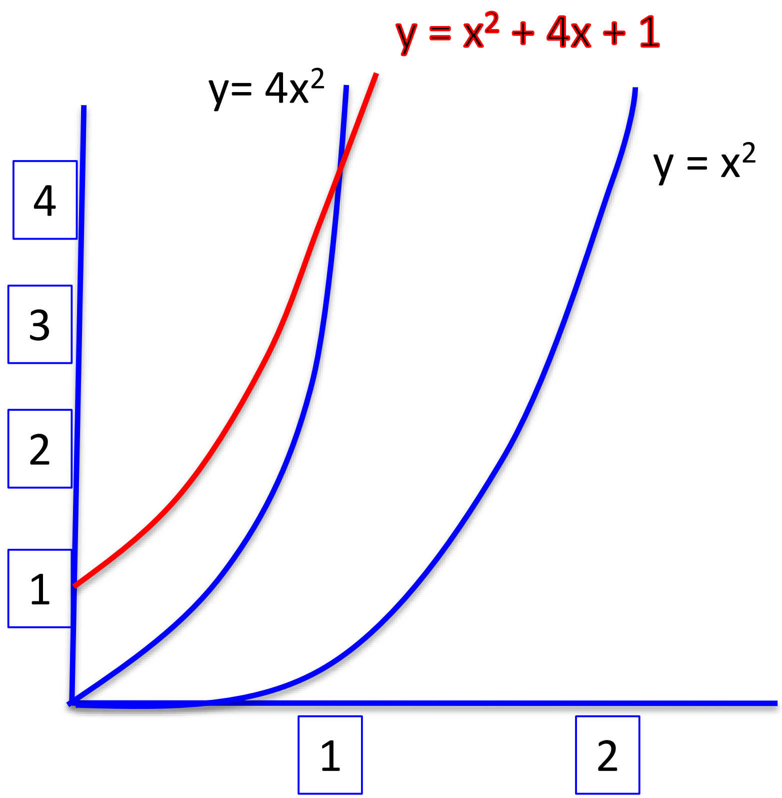
Intuitively, f(x) grows "slower than" some multiple of g(x) as x grows without bound. Thus O(g(x)) defines an upper bound of f(x).

Example. $7x^2 + 9x + 4$ is $O(x^2)$,

since $\mathbf{7x^2 + 9x + 4} \leq 4.\ x^2$ for all x

Thus C|g(x)| defines the Upper bound of the growth of a function

The Big-O notation



$x^2 + 4x + 1 = O(x^2)$

Since = $4\,x^2 > x^2 + 4x + 1$

whenever $x > 1$, $4x^2$ defines an upper bound of the growth of $x^2 + 4x + 1$

Defines an upper bound of the growth of functions

The Big-Ω (omega) notation

DEF. Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. Then f is $\Omega(g(x))$ if there are constants C and k, such that

$$|f(x)| \geq C|g(x)| \qquad \text{for all } x > k$$

Example. $7x^2 + 9x + 4$ is $\Omega(x^2)$,

since $\mathbf{7x^2 + 9x + 4} \geq 1.\ x^2$ for all x

Thus $C|g(x)|$ defines the lower bound of the growth of a function

Question. Is $7x^2 + 9x + 4$ $\Omega(x)$?`

The Big-Theta (Θ) notation

DEF. Let f and g be functions from the set of integers (or real numbers) to the set of real numbers. Then f is $\Theta(g(x))$ if there are constants C_1 and C_2 a positive real number k, such that

$$C1.|g(x)| \le |f(x)| \le C2.|g(x)| \qquad \text{for all } x > k$$

Example. $7x^2 + 9x + 4$ is $\Theta(x^2)$,

since $\mathbf{1.\,x^2} \le \mathbf{7x^2 + 9x + 4} \le \mathbf{8.\,x^2}$ for all $x > 10$

Average case performance

EXAMPLE. Compute the average case complexity of the ***linear search*** algorithm.

a_1 a_2 a_3 a_4 a_5 ..... a_n (Search for x from this list)

If x is the 1st element then it takes 3 steps

If x is the 2nd element then it takes 5 steps

If x is the i^{th} element then it takes (2i + 1) steps

So, the average number of steps = 1/n (3+5+7+…+2n+1) = ?

Classification of complexity

Complexity	**Terminology**
$\Theta(1)$	Constant complexity
$\Theta(\log n)$	Logarithmic complexity
$\Theta(n)$	Linear complexity
$\Theta(n^c)$	Polynomial complexity
$\Theta(b^n)$ $(b>1)$	Exponential complexity
$\Theta(n!)$	Factorial complexity

We also use such terms when Θ is replaced by O (big-O)

Greedy Algorithms

In optimization problems, algorithms that use the best choice at each step are called greedy algorithms.

Example. Devise an algorithm for making change for n cents using quarters, dimes, nickels, and pennies using the least number of total coins?

Greedy Change-making Algorithm

Let $c_1, c_2, \ldots, c_r$ be the denomination of the coins, and $c_i > c_{i+1}$

for i:= 1 to r
 while $n \geq c_i$
  begin
   add a coin of value c_i to the change
   $n := n - c_i$
  end

Question. Is this optimal? Does it use the least number of coins?

Let the coins be
1, 5, 10, 25 cents.
For making **38** cents,
you will use

1 quarter - 25
1 dime - 10
3 cents - 1

The total count is 5,
and it is optimum.

Greedy Change-making Algorithm

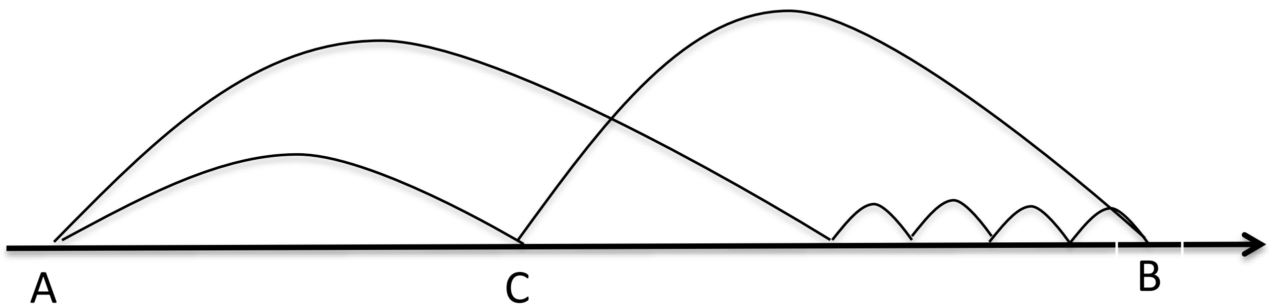
But if you don't use a nickel, and you make a change for **30** cents using the same algorithm, the you will use 1 quarter and 5 cents (total 6 coins). But the optimum is 3 coins (use 3 dimes!)

3 quarter - 10

1 quarter - 25
5 cents - 1

So, greedy algorithms produce results, but the results may be sub-optimal.

Greedy Routing Algorithm



If you need to reach point B from point A in the fewest number of hops,

Then which route will you take? If the knowledge is local, then you are

Tempted to use a greedy algorithm, and reach B in 5 hops, although

It is possible to reach B in only two hops.

Other classification of problems

- Problems that have polynomial worst-case complexity are called tractable. Otherwise they are called intractable.
- Problems for which no solution exists are known as unsolvable problems (like the halting problems). Otherwise they are called solvable.
- Many solvable problems are believed to have the property that no polynomial time solution exists for them, but a solution, if known, *can be checked in polynomial time*. These belong to the class NP [**nondeterministic polynomial time**](as opposed to the class of tractable problems that belong to class P [**nondeterministic polynomial time**])

The Halting Problems

The **Halting problem** asks the question.

Given a program and an input to the program, determine if the program will eventually stop when it is given that input.

Take a trial solution

- Run the program with the given input. If the program stops, we know the program stops.
- But if the program doesn't stop in a reasonable amount of time, then we cannot conclude that it won't stop. Maybe we didn't wait long enough!

Not decidable in general!

Chapter 4
Integers and Modular Arithmetic

Dr. Mohammed Marey

2018

Preamble

Historically, *number theory* has been a beautiful area of study in pure mathematics. However, in modern times, number theory is very important in the area of security. Encryption algorithms heavily depend on modular arithmetic, and our ability to deal with large integers. We need appropriate techniques to deal with such algorithms.

Divisibility and Modular Arithmetic

DEFINITION 1

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

77 | 7: false bigger number can't divide smaller positive number

7 | 77: true because 77 = 7 · 11

24 | 24: true because 24 = 24 · 1

1 | 2: true, 1 divides everything.

2 | 1: false.

0 | 24: false, only 0 is divisible by 0

24 | 0: true, 0 is divisible by every number (0 = 24 · 0)

THEOREM 1

Let a, b, and c be integers, where $a \neq 0$. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Example:

1. $17|34 \wedge 17|170 \rightarrow 17|204$
2. $17|34 \rightarrow 17|340$
3. $6|12 \wedge 12|144 \rightarrow 6 \mid 144$

COROLLARY 1

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

THEOREM 2 **THE DIVISION ALGORITHM** Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

DEFINITION 2 In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

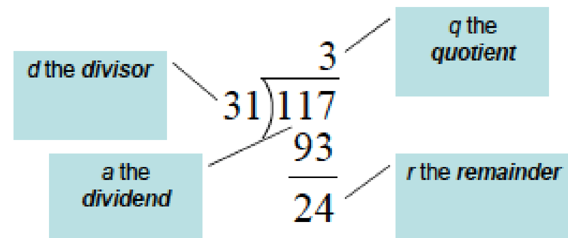
A: Compute

1. 113 **mod** 24:

$$\begin{array}{r} 4 \\ 24\overline{)113} \\ \underline{96} \\ 17 \end{array}$$

2. -29 **mod** 7

Remember long division?



117 = 31·3 + 24

a = *dq* + *r*

EXAMPLE 3 What are the quotient and remainder when 101 is divided by 11?

Solution: We have

$$101 = 11 \cdot 9 + 2.$$

EXAMPLE 4 What are the quotient and remainder when -11 is divided by 3?

Solution: We have

$$-11 = 3(-4) + 1.$$

DEFINITION 3 If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

THEOREM 3 Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \textbf{ mod } m = b \textbf{ mod } m$.

THEOREM 4 Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

THEOREM 5 Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

COROLLARY 2 Let m be a positive integer and let a and b be integers. Then

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

and

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m.$$

Primes and Greatest Common Divisors

DEFINITION 1 An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

THEOREM 1 **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

DEFINITION 2 Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

DEFINITION 3 The integers a and b are *relatively prime* if their greatest common divisor is 1.

DEFINITION 4 The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

DEFINITION 5 The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

factorizations of these integers. Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

THEOREM 5 Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

LEMMA 1 Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

EXAMPLE 16 Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$
\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41.
\end{aligned}
$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

ALGORITHM 1 The Euclidean Algorithm.

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return x{gcd(a, b) is x}
```

Let a = 12, b= 21

gcd (21, 12)
= gcd (12, 9)
= gcd (9, 3)

Since 9 mod 3 = 0
The gcd is 3

Prime Numbers

DEF: A number $n \geq 2$ ***prime*** if it is only divisible by 1 and itself. A number $n \geq 2$ which isn't prime is called ***composite***.

Q: Which of the following are prime?

0,1,2,3,4,5,6,7,8,9,10

Testing Prime Numbers

Prime numbers are very important in encryption schemes. Essential to be able to verify if a number is prime or not. It turns out that this is quite a difficult problem. First try:

```
boolean isPrime(integer n)
  if ( n < 2 ) return false
  for(i = 2 to n -1)
    if ( i |n )        // "divides"! not disjunction
      return false
  return true
```

Time Complexity

This algorithm has a time complexity O(n) (assuming that a|b can be tested in O(1) time). For an 8-digit decimal number, it is thus $O(10^8)$.

This is terrible. Can we do better?

Yes! Try only smaller prime numbers as divisors.

In fact, only need to try to divide by prime numbers no larger than $\sqrt{n}$ as we'll see next:

Greatest Common Divisor

Q: Find the following gcd's:

1. gcd(11,77)
2. gcd(33,77)
3. gcd(24,36)
4. gcd(24,25)

Q: Compute gcd (36, 54, 81)

(mod) Congruence

Q: Which of the following are true?

1. $3 \equiv 3 \pmod{17}$
2. $3 \equiv -3 \pmod{17}$
3. $172 \equiv 177 \pmod{5}$
4. $-13 \equiv 13 \pmod{26}$

Q: Compute the following.

1. 307^{1001} **mod** 102
2. $(-45 \cdot 77)$ **mod** 17
3. $$\left(\sum_{i=4}^{23} 10^i\right) \bmod 11$$

Modular Arithmetic: harder examples

A: Use the previous identities to help simplify:

1. Using multiplication rules, before multiplying (or exponentiating) can reduce modulo 102:

307^{1001} **mod** $102 \equiv 307^{1001} \pmod{102}$

$\equiv 1^{1001} \pmod{102} \equiv 1 \pmod{102}$. Therefore, 307^{1001} **mod** $102 = 1$.

A: Use the previous identities to help simplify:

2. Repeatedly reduce after each multiplication:

$(-45 \cdot 77)$ **mod** $17 \equiv (-45 \cdot 77) \pmod{17}$

$\equiv (6 \cdot 9) \pmod{17} \equiv 54 \pmod{17} \equiv 3 \pmod{17}$. Therefore $(-45 \cdot 77)$ **mod** $17 = 3$.

Chapter 5
Induction and Recursion

Dr. Mohammed Marey

2018

Mathematical Induction

- Proof methods: direct proof, proof by cases, proof by contraposition, proof by contradiction, disproof by counterexample

- Mathematical induction
  - very simple and powerful proof technique
  - often used to prove P(x) is true for all positive integers
  - "Guess" and verify strategy

Principle of Mathematical Induction

$$(P(1) \land \forall k(P(k) \rightarrow P(k+1)) \rightarrow \forall n P(n)$$

- To prove that $\forall n P(n)$, where $n \in Z^+$ and $P(n)$ is a propositional function, we complete two steps:
  - **1- Basis step:** Verify $P(1)$ is true
  - **2-Inductive hypothesis:**
  - **3-Inductive step:** Show $P(k) \rightarrow P(k+1)$ is true for arbitrary $k \in Z^+$

Mathematical Induction

- Knowing it is true for the first element means it must be true for the next element, i.e. the second element
- Knowing it is true for the second element implies it is true for the third and so forth.

$$\frac{P(1) \quad P(k) \rightarrow P(k+1)}{P(2)}, \quad \frac{P(2) \quad P(k) \rightarrow P(k+1)}{P(3)}, \quad \ldots$$

- Need a starting point (Base case)

- How to show P(1) is true?
  - Replace n by 1 in P(n)

- How to show P(k)→P(k+1) is true?
  - Direct proof is normally used
  - (Inductive Hypothesis) Assume P(k) is true for some arbitrary k
  - Then show P(k+1) is true

Proving Summation

- Example: Show that $1^2 + 2^2 + 3^2 + \ldots + n^2 = n(n+1)(2n+1)/6$, where $n \in Z^+$
- Proof:
  - **P(n):** $[1^2 + 2^2 + 3^2 + \ldots + n^2 = n(n+1)(2n+1)/6]$
  - **Basis case P(1):** LHS=$1^2 = 1$, RHS=$1*(1+1)(2*1+1)/6=1$
  - **Inductive hypothesis:** Assume P(k) is true:

    $1^2 + 2^2 + 3^2 + \ldots + k^2 = k(k+1)(2k+1)/6$
  - **Inductive step:** Prove P(k+1) is true
    - For P(k+1):

      Show that $1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$

      (Details on Board)
    - We showed P(k+1) is true under the assumption that P(k) is true.
  - By mathematical induction P(n) is true for all positive integers

Proving Inequalities

- Example: $n < 4^n$, where $n \in Z^+$
- Proof
  - **P(n):** $n < 4^n$
  - **Basis case: P(1)** holds since $1<4$
  - **Inductive hypothesis:** Assume P(k) is true: $k < 4^k$
  - **Inductive step:** Prove P(k+1) is true
    - For P(k+1):

      $k+1 < 4^k +1 < 4^k + 4^k = 2*4^k < 4*4^k = 4^{k+1}$
  - By mathematical induction P(n) is true for all positive integers

Proving divisibility

- Example: Prove that n^3-n is divisible by 3 whenever n is a positive integer.
  - **P(n):** n^3-n is divisible by 3 , n +ve integer
  - **Basis step:** P(1): $1^3-1=0$, which is divisible by 3.
  - **Inductive hypothesis:**

    Assume P(k) is true: $k^3 - k$ is divisible by 3
  - **Inductive step:** Prove P(k+1) is true
    - For P(k+1):

      $(k+1)^3 - (k+1)$

      $= k^3 + 3k^2 + 3k + 1 - k - 1$

      $= (k^3 - k) + 3(k^2 + k)$

      From the assumption, k^3-k is divisible by 3, so P(k+1) is true.

  By mathematical induction, P(n) is true for all positive integers

Mathematical Induction (Base case n≠1)

- Basis case doe not have to be n=1

- How to show that P(n) is true for n=b, b+1, b+2,.... where b is an integer other than 1?
  - i) Basis step: Verify P(b) is true
  - ii)Inductive step: Show $P(k) \rightarrow P(k+1)$ is true for arbitrary $k \in Z$

- Show that $1+2+2^2+...+2^n = 2^{n+1} -1$, where $n \in N$
- Proof by induction:
  - **P(n):** $1+2+2^2+...+2\ n = 2\ n+1\ -1$
  - **Basis step:** P(0): LHS=1, RHS = $2^1 -1 = 1$.
  - **Inductive hypothesis:** Assume P(k) is true for arbitrary $k \in N$, $1+2+...+2^k = 2^{k+1} -1$
  - **Inductive step:** Prove P(k+1) is true
    - Need to show P(k+1): $1+2+....+2^k+2^{k+1} = 2^{k+2} -1$ is true.

      LHS = $(1+2+...+2^k)+2^{k+1} = 2^{k+1}-1+2^{k+1} = 2^{k+2}-1$

      So LHS = RHS. We showed P(k+1) is true under the assumption that P(k) is true.
  - By mathematical induction P(n) is true for all natural numbers

- Prove $\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r-1}$ if $r \neq 1$
- Proof by induction:
  – **P(n):** $a+ar+ar^2 .... +ar^n = (ar^{n+1} -a)/(r-1)$
  – **Basis case:** P(0): a = (ar-a)/(r-1). So, P(0) is true
  – **Inductive hypothesis:** Assume P(k) is true for arbitrary k∈N, $a+ar+ar^2 .... +ar^k = (ar^{k+1} -a)/(r-1)$
  – **Inductive step:** Prove P(k+1) is true
    - Need to show P(k+1):
      $a+ar+ar^2 .... +ar^k + ar^{k+1} = (ar^{k+2} -a)/(r-1)$ is true.
    - LHS = $(ar^{k+1}-a)/(r-1) +ar^{k+1}$
      $= (ar^{k+1}-a +ar^{k+2} -ar^{k+1})/(r-1)$
    - So LHS = RHS.
    - We showed P(k+1) is true under the assumption that P(k) is true.
  – By mathematical induction P(n) is true for all natural numbers

Strong Induction

$$(P(1) \wedge \boxed{\forall k(P(1) \wedge P(2) \wedge \ldots \wedge P(k) \rightarrow P(k+1)))} \rightarrow \forall n P(n)$$

- To prove that $\forall n P(n)$, where $n \in Z^+$ and $P(n)$ is a propositional function, we complete two steps:
  - i) Basis step: Verify $P(1)$ is true
  - ii)Inductive step: Show $P(1) \wedge P(2) \wedge \ldots \wedge P(k) \rightarrow P(k+1)$ is true for arbitrary $k \in Z^+$

Strong Induction Variation

- A more general strong induction can handle cases where the inductive step is valid only for integers greater than a particular integer.

- To prove that $P(n)$ is true for all integer $n \geq b$, we complete two steps:
  - **1-Basis step:** Verify $P(b), P(b+1), \ldots, P(b+j)$ are true
  - **2-Inductive hypothesis:** Assume $P(j)$ is true for $b<j\leq k$ for an arbitrary $k>1$
  - **3-Inductive step:** Show $P(b+1) \wedge P(b+2) \wedge \ldots \wedge P(b+k) \rightarrow P(k+1)$ is true for every integer $k \geq b+j$

- Example: Show that if n is an integer greater than 1, then n can be written as the product of primes
- Proof by strong induction:
  - First identify P(n), P(n): n can be written as the product of primes
  - **Basis step:** P(2): 2 is a prime number, so P(2) is true.
  - **Inductive hypothesis:** Assume P(j) is true for $1<j\leq k$ for an arbitrary $k>1$, i.e. j can be written as the product of primes when $1<j\leq k$
  - **Inductive step:** Prove P(k+1) is true
    - Need to show P(k+1).
      - Case 1: k+1 is prime, then P(k+1) is true.
      - Case 2: k+1 is composite

        $k+1=a*b$, where a and b are positive integers, and $2\leq a,b\leq k$.

        By the assumption, a and b can be written as the product of primes. Then k+1 can be written as the product of primes.

Example

- Show that every postage amount 12 cents or more can be formed using only 4 and 5 cent stamps

Proof using Mathematical Induction

- Show base case: P(12):
  - 12 = 4 + 4 + 4
- Inductive hypothesis: Assume P(k) is true
- Inductive step: Show that P(k+1) is true
  - If P(k) uses a 4 cent stamp, replace that stamp with a 5 cent stamp to obtain $P(k+1)$
  - If P(k) does not use a 4 cent stamp, it must use only 5 cent stamps
    - Since $k > 10$, there must be at least three 5 cent stamps
    - Replace these with four 4 cent stamps to obtain k+1
- Note that only $P(k)$ was assumed to be true

Same Proof using Strong Induction

- Show base cases: P(12), P(13), P(14), and P(15)
  - $12 = 4 + 4 + 4$
  - $13 = 4 + 4 + 5$
  - $14 = 4 + 5 + 5$
  - $15 = 5 + 5 + 5$
- Inductive hypothesis: Assume P(k-3), P(k-2), P(k-1), P(k) are all true
  - For $k \geq 15$
- Inductive step: Show that P(k+1) is true
  - We will obtain P(k+1) by adding a 4 cent stamp to P(k+1-4)
  - Since we know P(k+1-4) = P(k-3) is true, our proof is complete
- Note that P(k-3), P(k-2), P(k-1), P(k) were all assumed to be true

Mathematical Induction example

Prove that a set with n elements has 2^n subsets.

1-Hypothesis: set with n elements has 2^n subsets

2- Base case (n=0): $S=ø$, $P(S) = \{ø\}$ and $|P(S)| = 1 = 2^0$

3- Inductive Hypothesis - P(k): given $|S| = k$, $|P(S)| = 2^k$

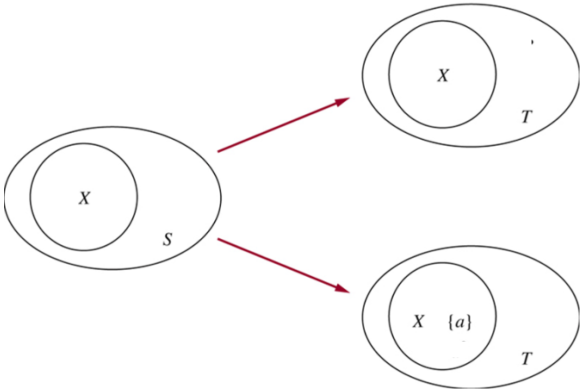
4- Inductive Step: $\forall(k)\ P(k) \rightarrow P(k+1)$, assuming P(k). i.e,
Prove that if $|T| = k+1$, then $|P(T)| = 2^{k+1,}$ given that $P(k)=2^k$

Inductive Step: Prove that if $|T| = k+1$, then $|P(T)| = 2^{k+1}$ assuming P(k) is true.

$T = S \cup \{a\}$ for some $S \subset T$ with $|S| = k$, and $a \in T$

How to obtain the subsets of T?

For each subset X of S there are exactly two subsets of T, namely X and $X \cup \{a\}$



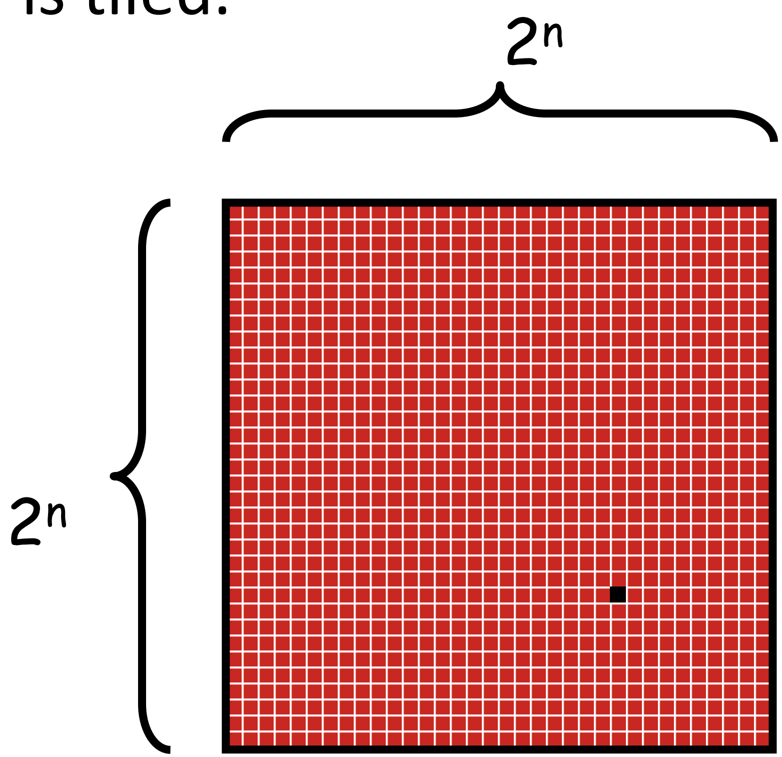
Generating subsets of a set T with k+1 elements from a set S with K elements

Because there are 2^k subsets of S (why?), there are 2×2^k subsets of T.

Ind. hypothesis

Deficient Tiling

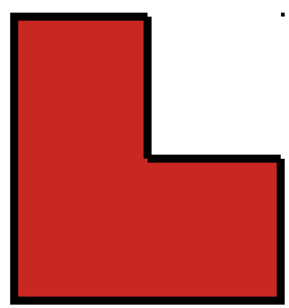
- A 2^n x 2^n sized grid is *deficient* if all but one cell is tiled.



Mathematical Induction - a clever example

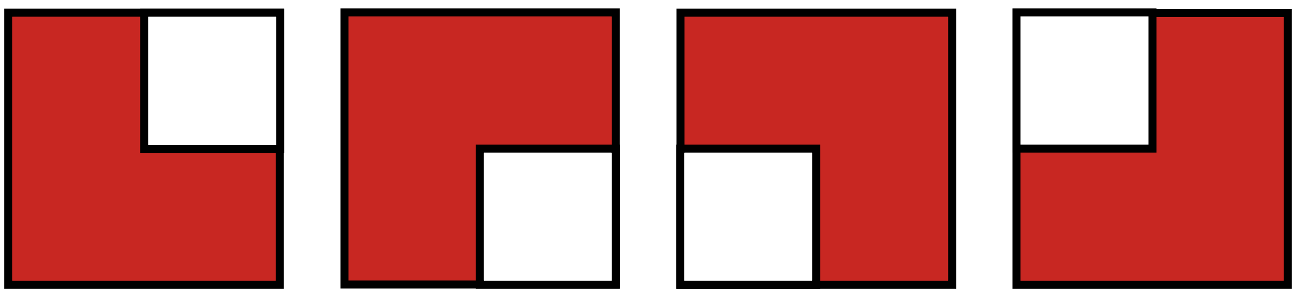
Hypothesis:

P(n) - We want to show that all 2^n x 2^n sized deficient grids can be tiled with right triominoes, which are pieces that cover three squares at a time, like this:



- **Base Case:**

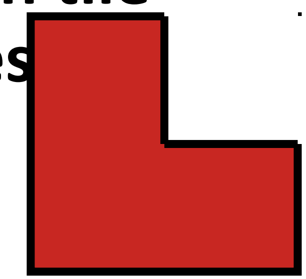
P(1) - Is it true for $2^1 \times 2^1$ grids?

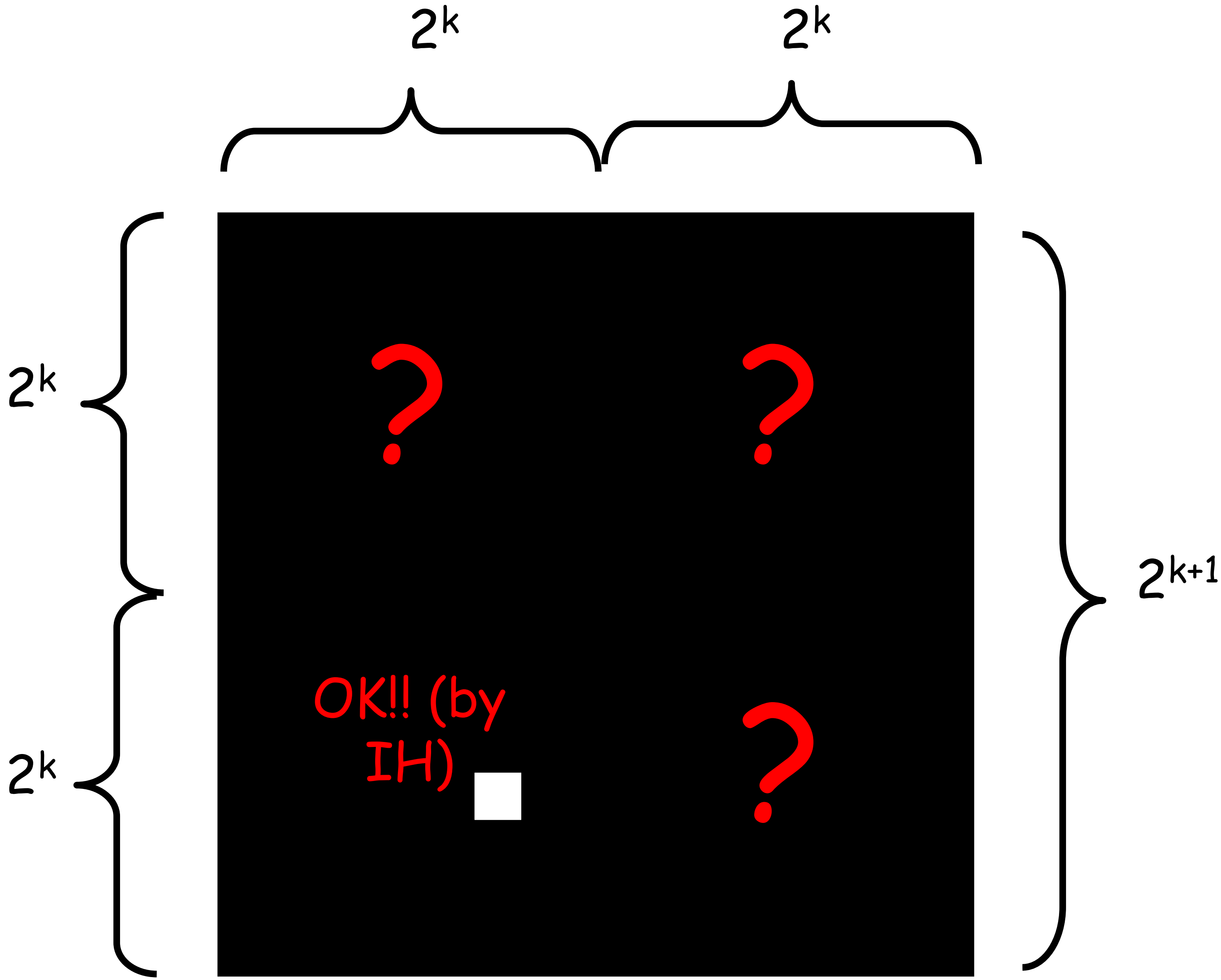


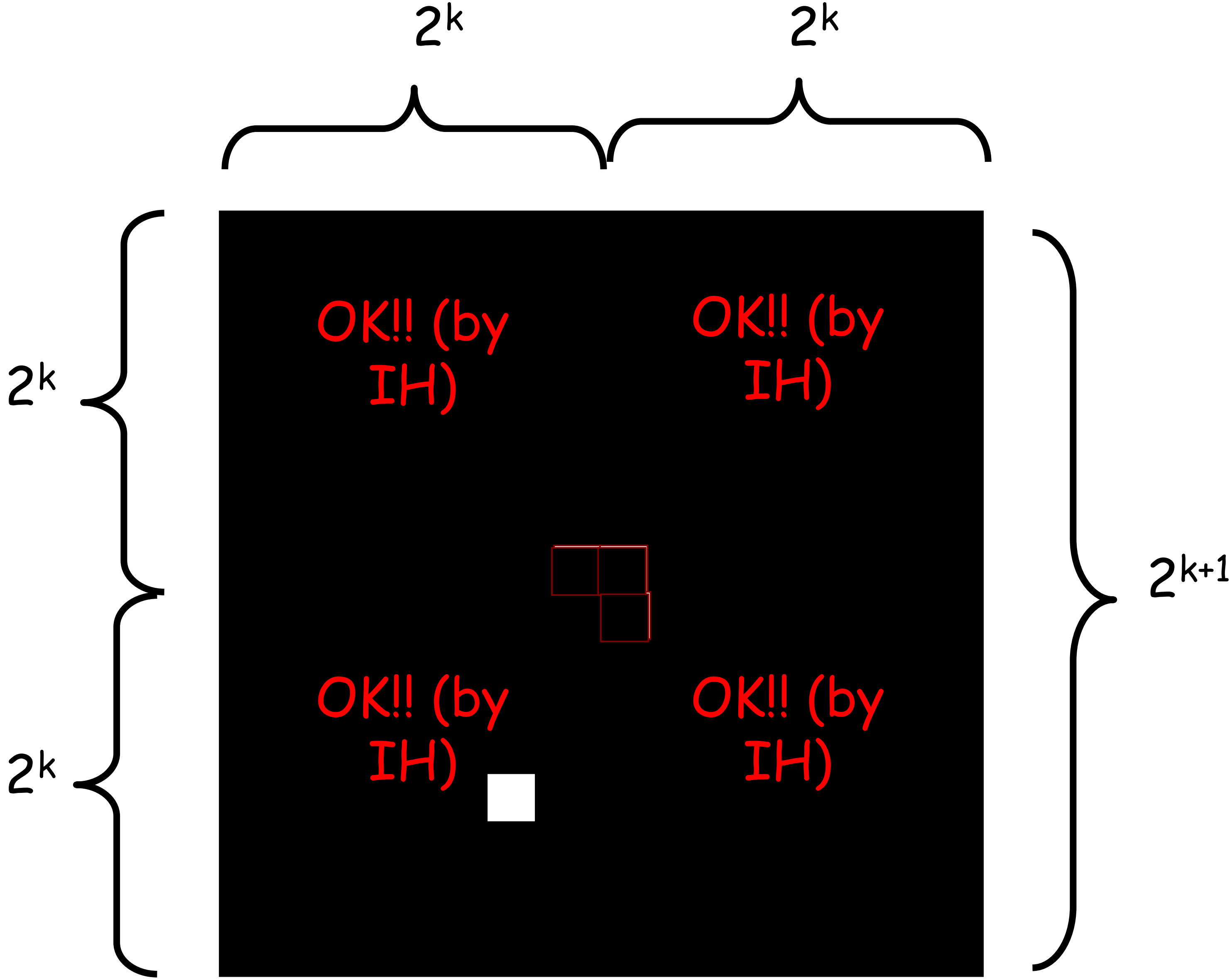
YES

- **Inductive Hypothesis:**
- **We can tile a 2^k x 2^k deficient board using our designer tiles.**

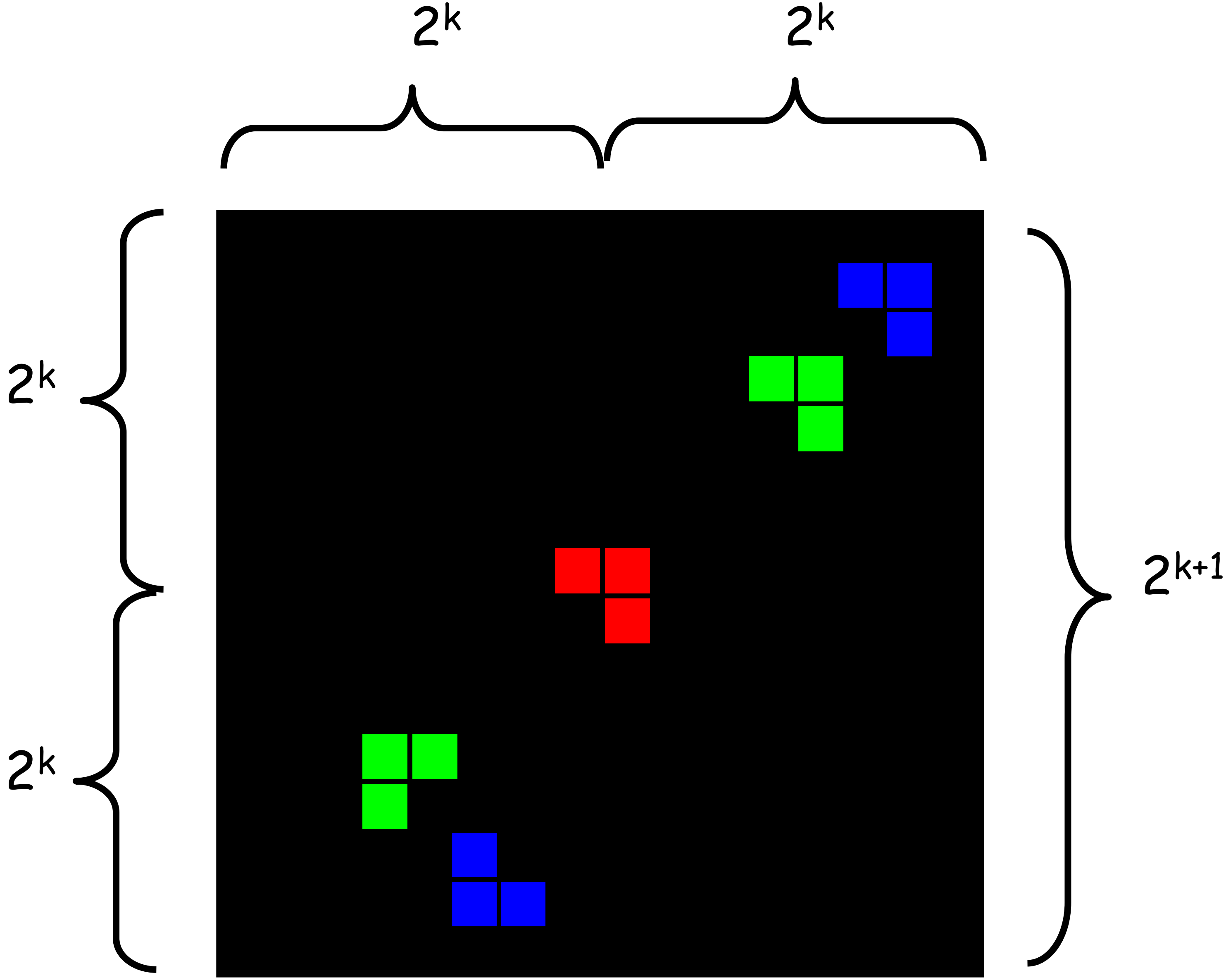
- **Inductive Step:**
- **Use this to prove that we can tile a 2^{k+1} x 2^{k+1} deficient board using our des**



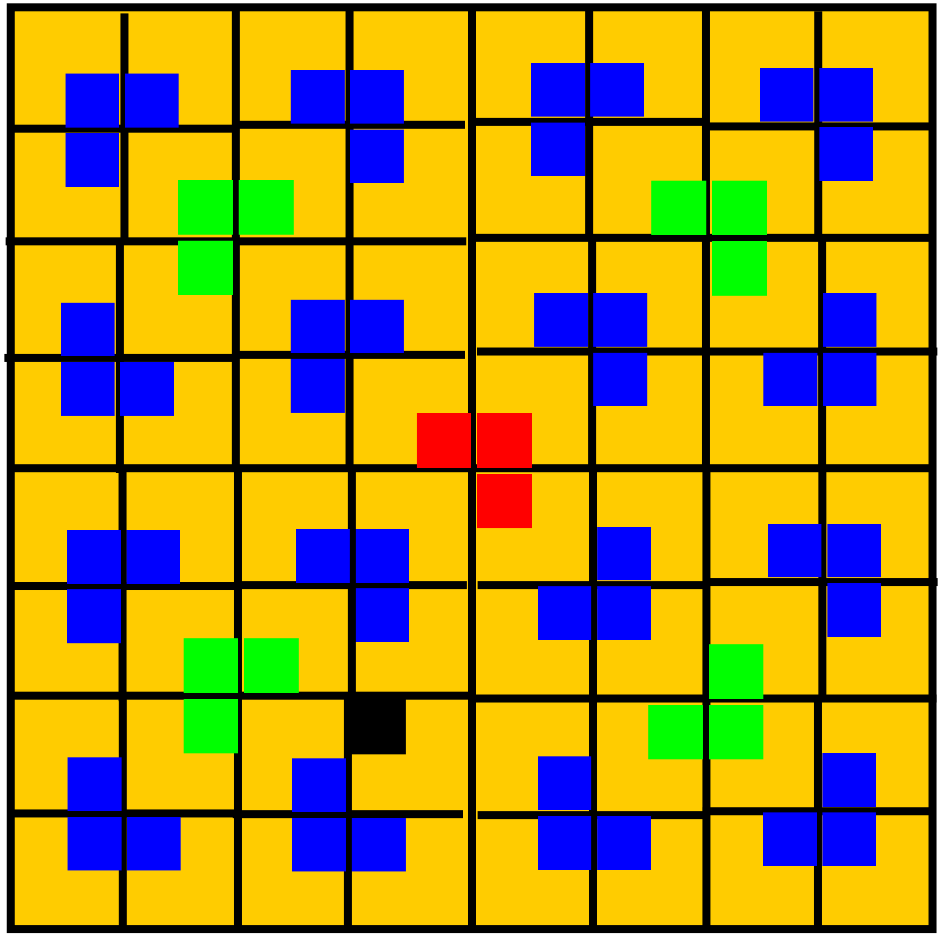

2^k
2^k
2^k
2^k
2^{k+1}
?
?
OK!! (by IH)
?



2^k
2^k
2^k
2^k
2^k+1
OK!! (by IH)
OK!! (by IH)
OK!! (by IH)
OK!! (by IH)


2k
2k
2k
2k
2k+1

So, we can tile a $2^k \times 2^k$ deficient board using our designer tiles.



What does this mean for 2^{2k} mod 3? **= 1** (also do direct proof by induction)

Thanks