Five Worlds: a Mathematical Problem Determines Which One We Live In

Olga Kharlampovich

December 7

Computation

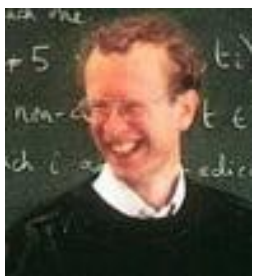
Computation: every process which is a sequence of simple steps, that we want to perform, or understand

There is essential computational component in a variety of natural phenomena.

Computation in math

Solving equations: $x^2 + y^2 = z^2 \Rightarrow$ Solution $x = 3,\ y = 4,\ z = 5$

Proving theorems: $x^n + y^n = z^n, n > 2 \Rightarrow$ **NO solution, Great Fermat Theorem proved by Wiles** 200 pages paper



Can we prove theorems automatically?

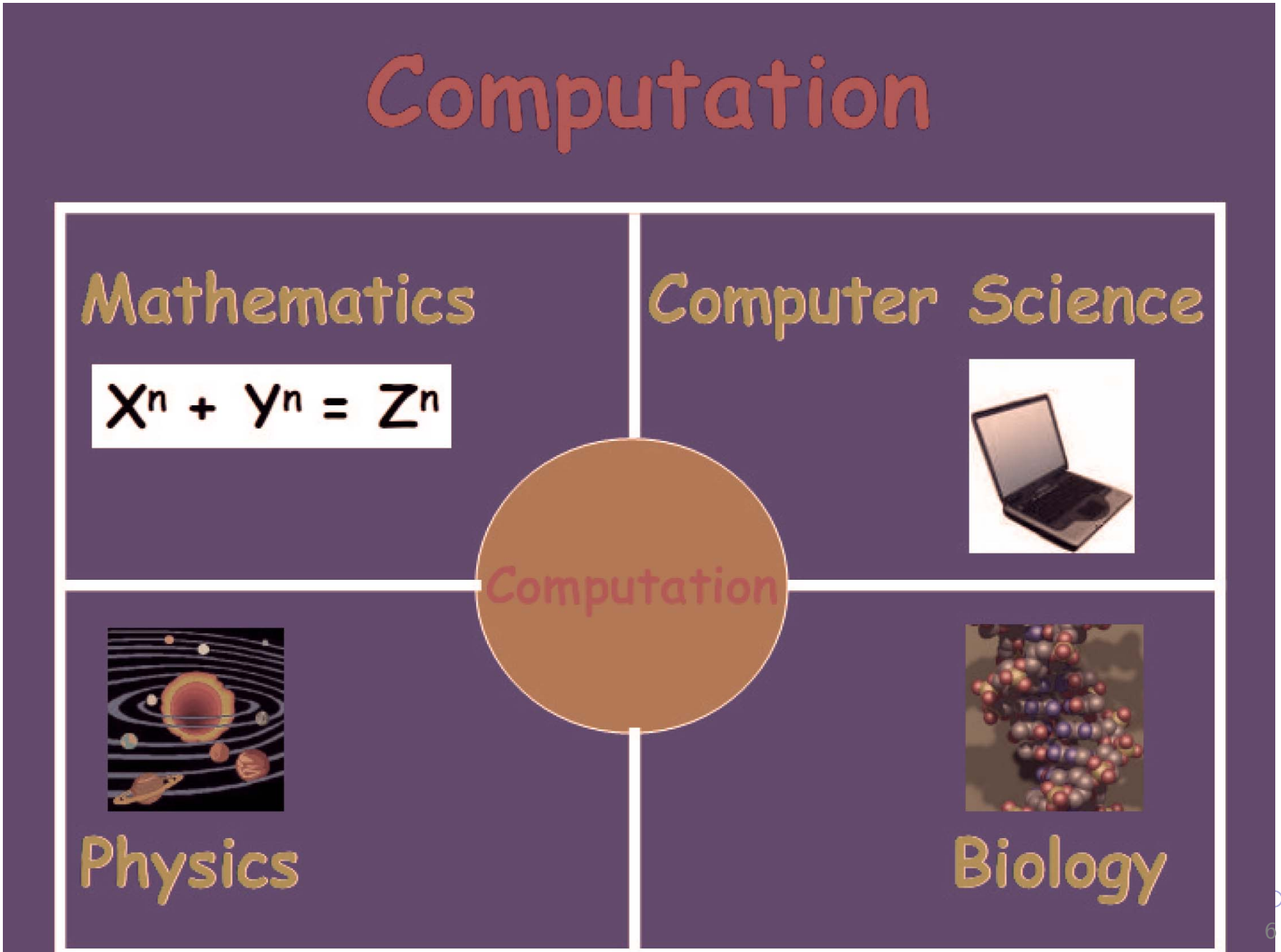
Computation in nature

Fetal development - Nature computes! In nature a computation is an evolution of an environment via repeated application of simple rules or processes.

Computation in love

FINDINGS

Hitting It Off, Thanks to Algorithms of Love


Computation
Mathematics
$X^n + Y^n = Z^n$
Computer Science
Computation
Physics
Biology

Plan

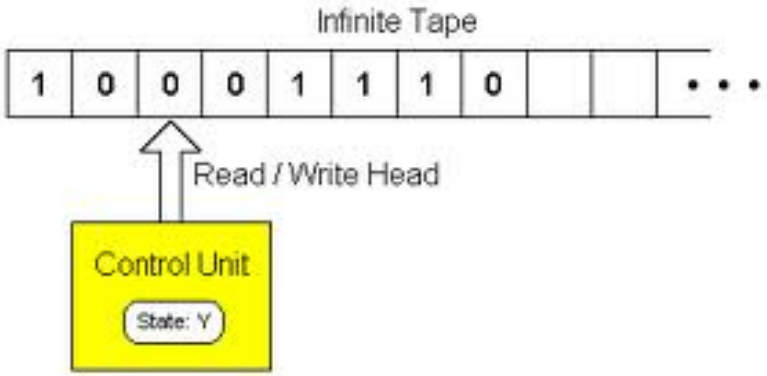
- We live in the universe where computation plays an important role.
- From Google to Genomics, the notion of an algorithm underlies this universe. Algorithm is the language of computation.
- Fast algorithms: P
- Fast verification: NP
- Is P=NP? (Is to find harder than to verify?)
- Hard problems are useful: Public key cryptography
- Five worlds of Russell Impagliazzo

Algorithm

Alan Turing 1912-1954

Formal definition of algorithm (Turing machine =computer with infinite memory)

Church-Turing Thesis: everything that can be computed in nature can be done on a Turing machine.



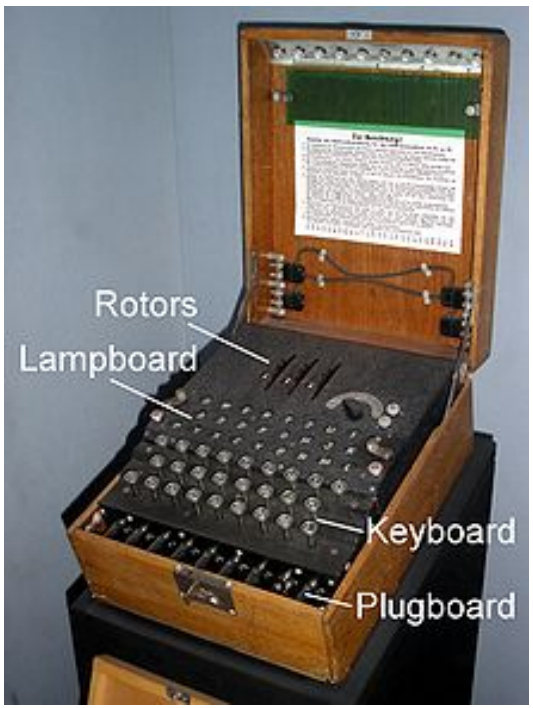
Limits on the power of algorithms

There is no algorithm to decide if a given computer program P halt on all inputs

There is no algorithm to decide if a given integer equation has an integer solution

Interesting to know

Alan Turing was the key player in the breaking of the German Enigma code at Bletchley Park during World War II.



Algorithm

Efficiency of an algorithm: number of basic steps for larger and larger inputs

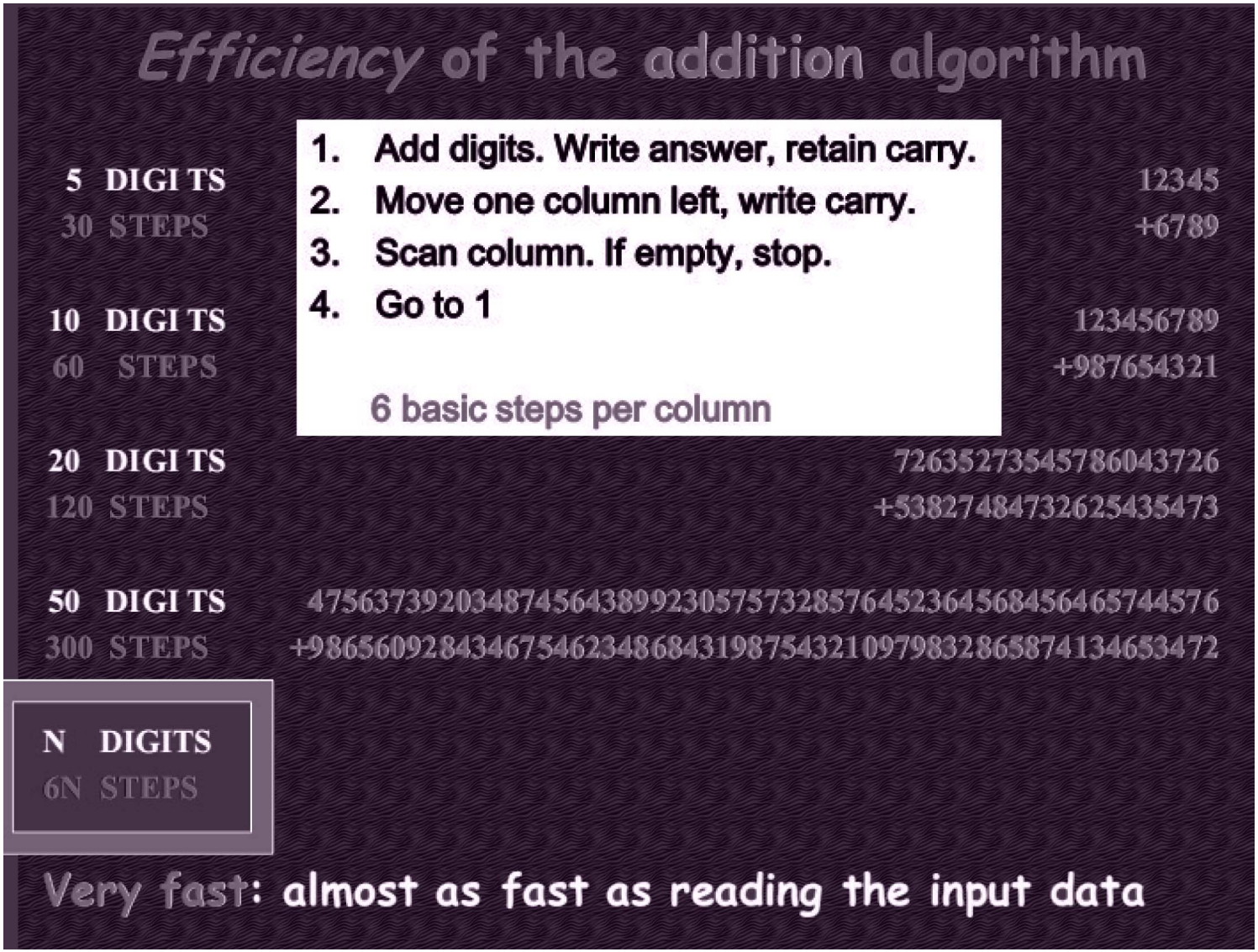
Example: Rubik's cube


n=2


n=3


n=4


n=5



pages 10-12 are from Wigderson's presentation PvsNP

Efficiency of the multiplication algorithm

5 DIGITS
25 STEPS

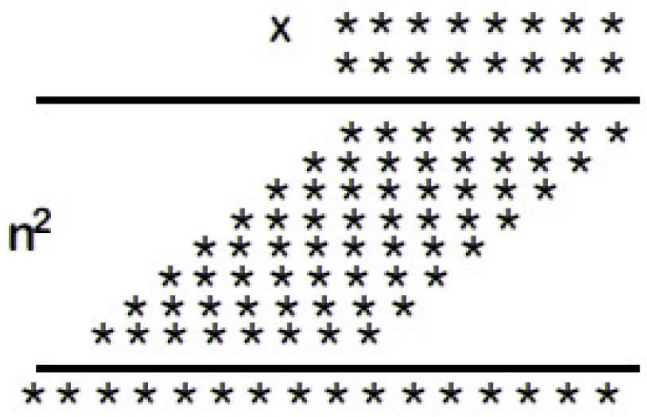
10 DIGITS
100 STEPS

20 DIGITS
400 STEPS

50 DIGITS
2500 STEPS

N DIGITS
N^2 STEPS

Grade-school multiply algorithm



12345
x6789

123456789
x 987654321

726352735457860437 26
x5382748473262543 5473

475637392034874564389923057573285764523645684564 65744576
986560928434675462348684319875432109798328658741 34653472

Fast! Multiply 10,000 digits in a second!

Is there a faster algorithm?

Efficiency of a factoring algorithm

? × ? = 147,573,952,588,676,412,927

Find nontrivial factors of a number A

N DIGITS

$10^{N/2}$ STEPS

Brute force factoring algorithm

Input: A

- For B = 2,3,…√A do:
- If B divides A, return B, A/B

Very slow! 1000 digits → sun will die before finishing

Is there a faster algorithm?

Yes, but still extremely slow!

Algorithm

Addition and multiplication is easy!

Is factoring hard? slow?

We don't know

The class P

The class P is the class of all problems having an efficient algorithm to find solutions

(efficient algorithm is a polynomial time algorithm, namely the number of steps to do computation for N digit numbers is bounded by N or N^2 or N^3 etc.)

Many interesting problems are in P

Addition and multiplication algorithms are in P

We will mention other examples of efficient algorithms:

Efficient algorithms: Error correction codes

Reed-Solomon decoding, 60

Petersen 60

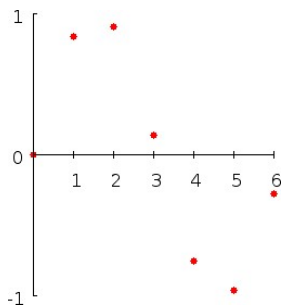
Berlecamp-Massey 68

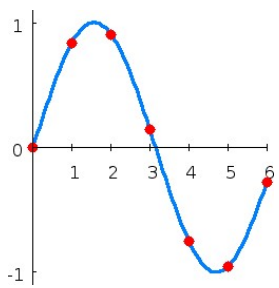
CDs, DVDs

Satellite communication

Cell phones

Paper bar codes (printed at home tickets etc.)





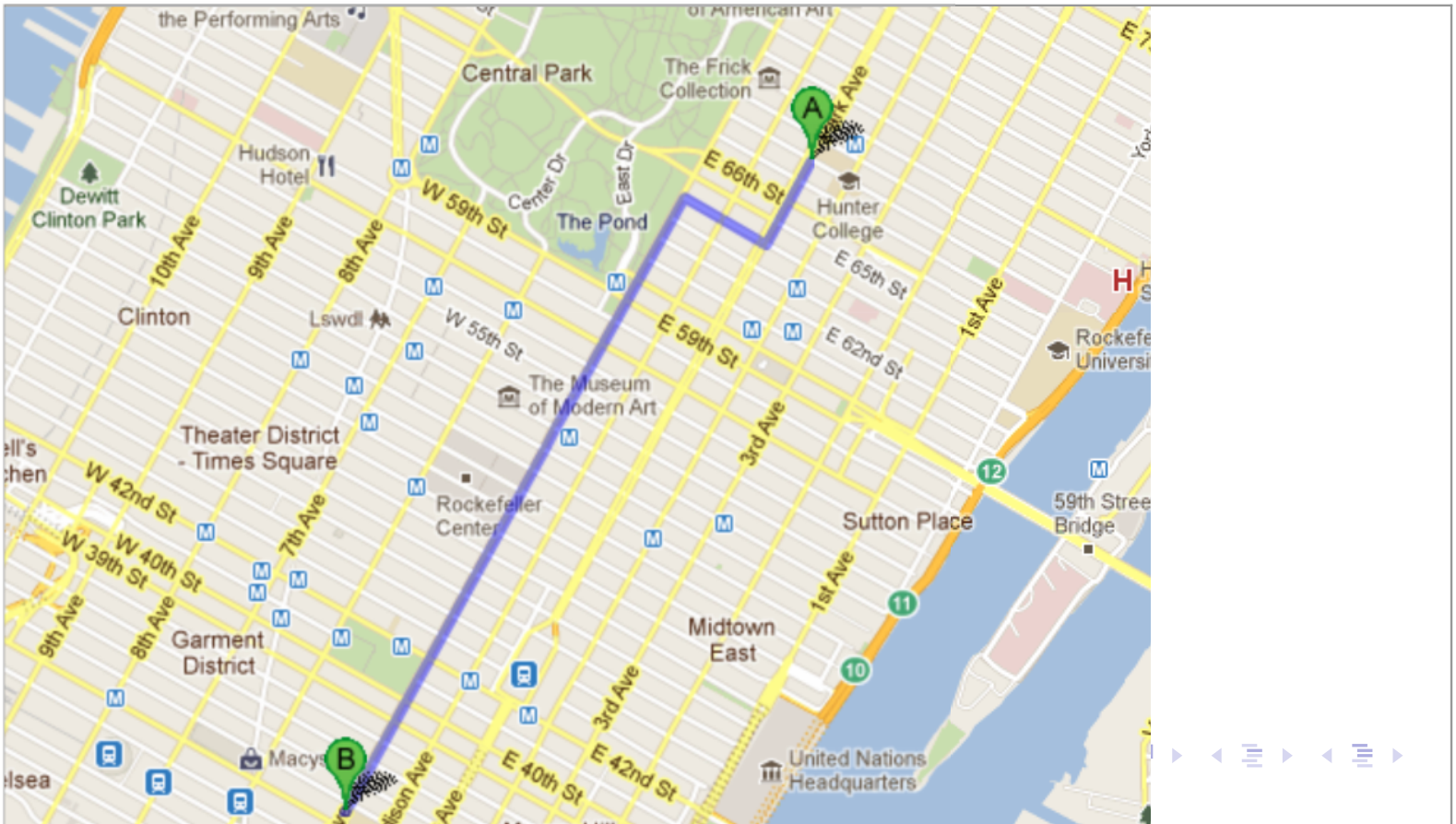
Efficient algorithms: Shortest path

Dijkstra, 1959

695 Park Ave, New York, NY 10065 to 365 5th Ave, New York, NY 10016 - Google ... Page 1 of 1

Google

To see all the details that are visible on the screen, use the "Print" link next to the map.



Efficient algorithms: Pattern matching

Rabin-Karp string search algorithm
Knuth-Morris-Pratt algorithm, 1977
Boyer-Moore string search algorithm, 1977

Text processing, Spell checking
Web search

Genome, Molecular biology

Efficient algorithms changed our life

YOU KNOW YOU ARE LIVING IN 2011 when...

1. You accidentally enter your PIN on the microwave.
2. You e-mail the person who works at the desk next to you.
3. You pull up in your own driveway and use your cell phone to see if anyone is home to help you carry in the groceries...
4. Every commercial on television has a web site at the bottom of the screen
5. Leaving the house without your cell phone, which you didn't even have 10 years ago, is now a cause for panic and you turn around to go and get it
6. You get up in the morning and go on line before getting your coffee
7. You start tilting your head sideways to smile. :)

The class NP (non-deterministic polynomial)

Are all interesting problems in P?

Cook, Levin 1971, and earlier, Godel 1956

The class NP is the class of all problems having efficient verification algorithms of given solutions

For each such problem, it is, maybe, hard to find a solution, but if somebody gives you a solution it takes polynomial time to verify that it is, indeed, a solution.

The class NP (non-deterministic polynomial)

Examples of problems in NP:
1. All problems that are in P;
2. Can a map be colored by three colors?
3. Sudoki game.

For each such problem, finding a solution (of length n) takes $\leq 2^n$ steps: try all possible solutions and verify each.

Can we do better? Do all NP problems have efficient algorithms?
Is P=NP?
Conjecture: P$\neq$ NP.
A problem is NP-complete if finding a polynomial algorithm for its solution would imply $P = NP$. (Factoring is NOT NP-complete)

Are hard problems (like factoring) useful?

YES! Hard problems are useful in public key cryptography

During the early history of cryptography, two parties would rely upon a key using a secure, but non-cryptographic, method; for example, a face-to-face meeting or an exchange via a trusted courier. This key, which both parties kept absolutely secret, could then be used to exchange encrypted messages. A number of significant practical difficulties arise in this approach to distributing keys.

Radio

In 1909, Marconi and Karl Ferdinand Braun were awarded the Nobel Prize in Physics for "contributions to the development of wireless telegraphy".

$\Rightarrow$ A need for Public key cryptography

Public-key cryptography: users can communicate securely over a public channel without having to agree upon a shared key beforehand.

Public key cryptography

Diffie, Hellman, Merkle (1974)

Public key cryptography

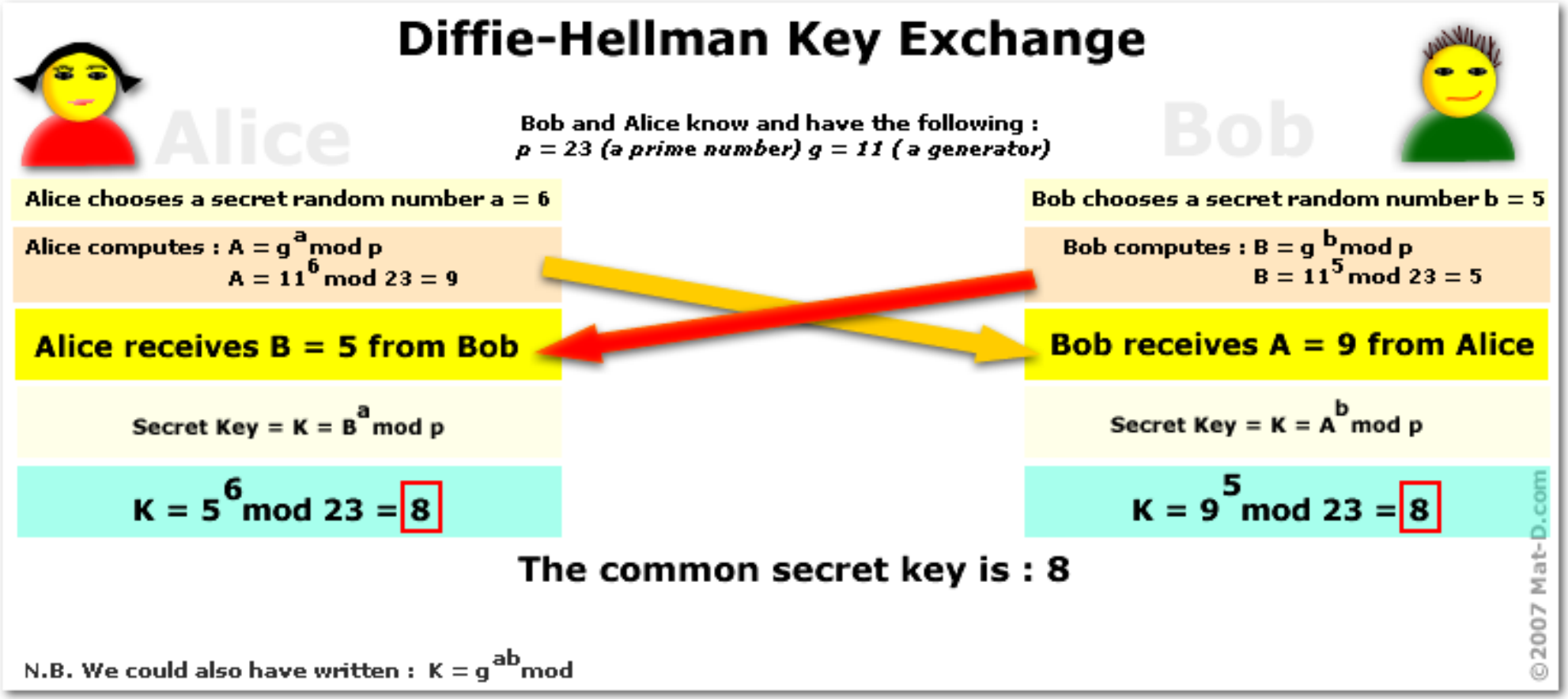
Alice and Bob publish number g (a generator)

Alice has secret number a, Bob has secret number b.

Alice publishes g^a, Bob publishes g^b.

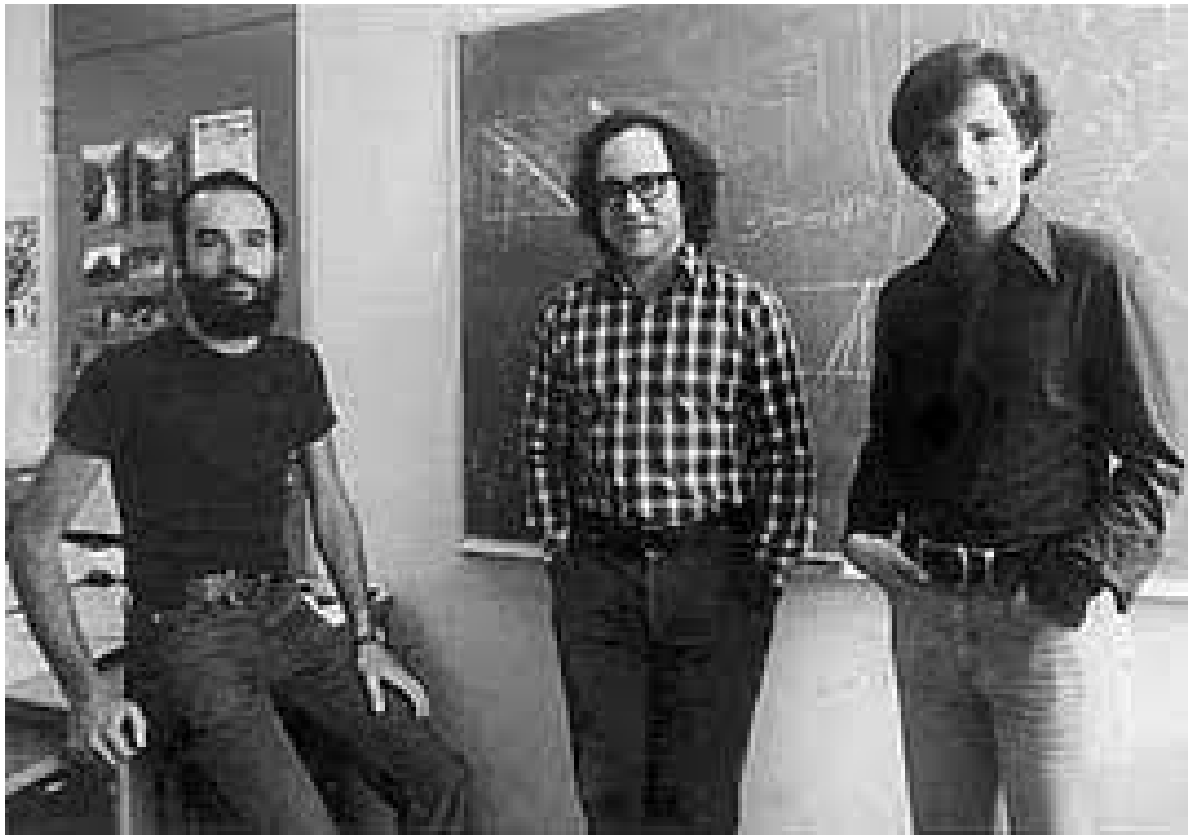
Now they have a secret key $g^{ab} = (g^a)^b = (g^b)^a$.

The rest of the world (Eve) has to find a or b, $a = log_g(g^a)$ but it takes long time to compute logarithm.

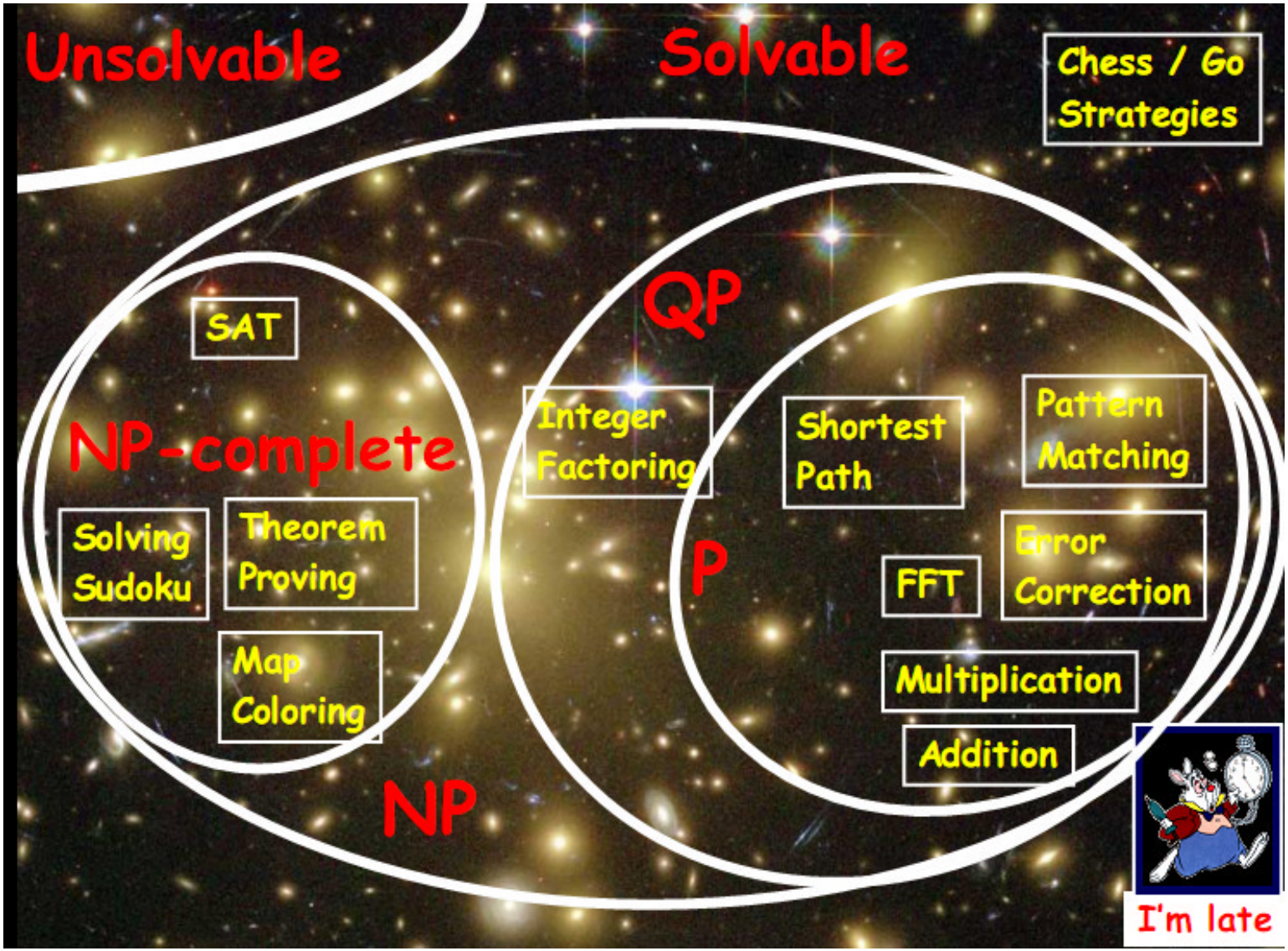

Diffie-Hellman Key Exchange
Alice
Bob
Bob and Alice know and have the following :
p = 23 (a prime number) g = 11 (a generator)
Alice chooses a secret random number a = 6
Bob chooses a secret random number b = 5
Alice computes : A = g^a mod p
A = 11^6 mod 23 = 9
Bob computes : B = g^b mod p
B = 11^5 mod 23 = 5
Alice receives B = 5 from Bob
Bob receives A = 9 from Alice
Secret Key = K = B^a mod p
Secret Key = K = A^b mod p
K = 5^6 mod 23 = 8
K = 9^5 mod 23 = 8
The common secret key is : 8
N.B. We could also have written : K = g^ab mod
©2007 Mat-D.com

Public key cryptography

Rivest, Shamir, and Adleman (RSA)



Universe by A. Wigderson



Five worlds

Russell Impagliazzo wrote a survey on Average-Case Complexity describing 5 possible worlds: we live in one of them, but do not yet know which one.

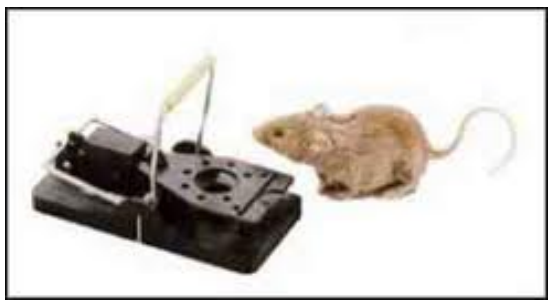
Algorithmica is the world in which $P = NP$. Utopia! Lots of science, math, engineering problems can be automated. No cryptography, no secrets, no internet exams.

If P=NP we have fast, automated finder.

Heuristica is the world where NP problems are intractable in the worst case but tractable on average, the same Utopia!

Five worlds

$y = f(x)$ is one way function if given x it is easy to find y, but knowing y is hard to find x. Multiplication, Discrete logarithm are, probably, such functions.



Pessiland is the world in which there are hard average-case problems, but no one-way functions. This is the worst possible world.

Five worlds

Minicrypt is the world in which one-way functions exist, but public-key cryptography is impossible.

Cryptomania is the world in which public-key cryptography is possible. Electronic commerce, secure e-mail, on-line exams.

Hopefully, we live in this world.

Millenium Prize Problems by Clay Math Institute

P versus NP problem
Hodge conjecture
Riemann hypothesis
Yang-Mills existence and mass gap
Navier-Stokes existence and smoothness
Birch and Swinnerton-Dyer conjecture
Poincaré conjecture (solved!)