Lecture Notes

Foundations of informatics — a bridging course
Mathematical tools

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Fall 2014

©2014 Michael Nüsken

Foundations of informatics — a bridging course
Fall 2014
Mathematical tools

MICHAEL NÜSKEN

1. Lights and cards

Exercise 1.1 (Lights on). (10 points)

You are left in a large round hall. In it you discover a circle of lamps. At the wall below each lamp is a switch. Yet, you discover that each switch changes the on/off-status of the lamp and its left and right neighbor. Unattainable for you in the middle of the room is a mechanism that can open the only exit. Yet, it opens only if the room is completely lit, ie. all lights are on.

(i) Your particular room has 4 lamps, and the first and second are lit. 2

(ii) Your room has 6 lamps, and the first and third are lit. 3

(iii) Develop and describe a general procedure to escape. 5

Exercise 1.2 (Cards dealt). (10 points)

Consider a simple game: n players are sitting in a round. Player i has v_i cards. She may give $2k$ cards away, half to the left and half to the right. The team wins when finally all players have a multiple of m cards.

The problem corresponds to distributing the load of a large bunch of given jobs to n computing centers, where each single machines can run m jobs. However, since sending data is expensive data can only be transferred to a neighboring center. To avoid conflicts between the neighbors, both neighbors shall get the same amount of additional jobs. Since starting a machine for less than m jobs is much more expensive than giving that to neighboring centers, the aim is to have a multiple of m jobs.

(i) Say $n = 3$, $m = 4$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. 3

(ii) Say $n = 3$, $m = 5$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. 3

(iii) Say $n = 4$, $m = 7$, and $v_1 = 2$, $v_2 = 5$, $v_3 = 11$, $v_4 = 3$. 4

Exercise 1.3 (A strange treasure). (15 points)

Five beagle boys have finally succeeded in stealing some of Scrooge McDuck gold dollars. They decide that they will split up their treasure the next morning. 15

During the night the first beagle boy wakes up and thinks to himself: Well, better I take my share now. He counts the coins and notices that the number divides by five only after removing one coin which he throws away. Then he takes his share and goes to sleep again.

Well, this repeats for the other four beagle boys as well.

Next morning, the five divide the remaining coins equally among them without any spare coin.

How many coins did the treasure have at the beginning? (And how many coins did each of them get?) Find the smallest answer. Find all answers.

Lights on!

brico
7.10.14
(1)

Vlad: Translate to binary form.

Lamp states: on = 1,
off = 0.

Encode operations and ...

Abdullah:

... found by trial (and error).

ALbi: A XOR B → ~~A×B+1~~

1 1 → 0

0 1 → 1

1 0 → 1

0 0 → 0

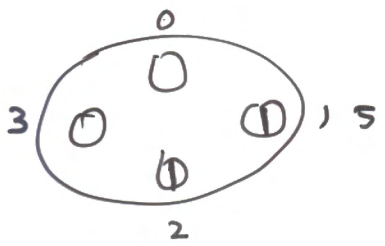
~~A B → A+B~~

a b → a+b

Michael: Does the order of operations (moves) matter?

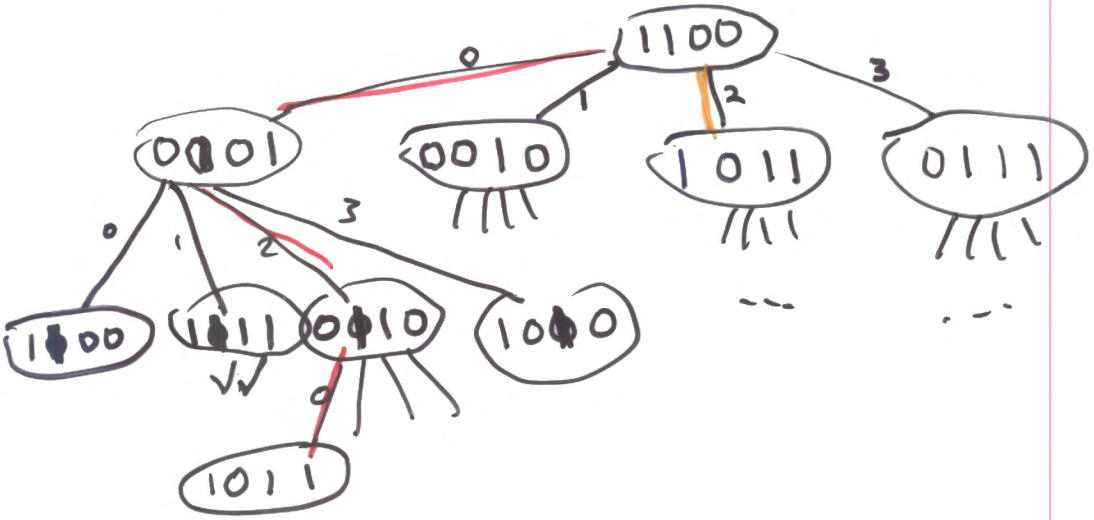
Abdullah: Do we ever need to operate a switch more than once?

Farshid:



1100

mod(4,4)



Chik-yuk:

$$\begin{array}{rl} 101000 & \leftarrow l \\ 001110 & \leftarrow x \\ \hline 100110 & \leftarrow l' \end{array}$$

XOR

Input Array l

Array x

Output Array l'

for ($i=0$ to length(l)

$l'[i] = l[i] \oplus x[i]$

$l \oplus a \oplus b$ $\quad$ $a \oplus l \oplus b$

$\Leftrightarrow l \oplus b \oplus a$.

$$\begin{array}{rl} & 001110 \\ l \oplus a \oplus a \quad \otimes & 001110 \\ \hline & 000000 \end{array}$$

brico
7.10.14
2

Excursion $\mathbb{Z}_2 = (\{0,1\}, +)$

don't PANIC !

Proper: Input: $a, b \in \{0,1\}$
Output: $c \in \{0,1\}$

a	b	c
0	0	0
0	1	1
1	0	1
1	1	0

$+ : \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}$

Group

Associative $\forall a,b,c \in \{0,1\}: (a+b)+c = a+(b+c)$

Proof: Inspect.

Neutral element: $\exists 0\ \forall a: \quad a+0 = a \quad *$
$0+a = a$

Proof: Inspect.

Inverses: $\forall a\ \exists b: \quad a+b = 0,$
$b+a = 0.$

Commutative

Commutative: $\forall a,b: \quad a+b = b+a.$

Consequence:

General associativity and commutativity:

e.g.: $a+b+c+\dots+z = z+\dots+a+c+b$

Meta question: Does the order of moves matter?

No: because the operation on arrays of bits given by the coordinate-wise XOR (addition) is associative and commutative.

Meta question 2 (Abdullah): No move needs to be repeated...

brico
7.10.14

Translations:

- Lamp state: on = 1, off = 0.
- Switch operation: 1 = change, 0 = don't change.

Array of bits = Lamps state

Array of bits = Move (one active operation of a switch)

Array of bits = Game solution (indicator of how often a switch is used)

Four lamps example:

initial state: $e = (1100) = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ (lamp 0, lamp 1, ...)

all moves: $M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ (switch 0, switch 1, ...)

general for:

game solution: $x = \begin{bmatrix} x_0 \\ \vdots \\ x_3 \end{bmatrix}$, $x_i = 0$ if switch i is unused

$x_i = 1$ if switch i is used.

final state: $e' = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = e + M \cdot x$ (target)

$e + M \cdot x$ is state after x

Excursion $\mathbb{F}_2 = (\{0,1\}, +, \cdot)$

P: $\cdot : \{0,1\} \times \{0,1\} \to \{0,1\}, (a,b) \mapsto a \cdot b$ (= ab)

a \ b	0	1
0	0	0
1	0	1

← $a \cdot b$

A: $(ab)c = a(bc)$

N: $1a = a, \quad a \cdot 1 = a$

I: $\forall a \neq 0 \ \exists b: \quad ab = 1, \quad ba = 1.$

C: $ab = ba.$

D: $(a+b) \cdot c = a \cdot c + b \cdot c,$

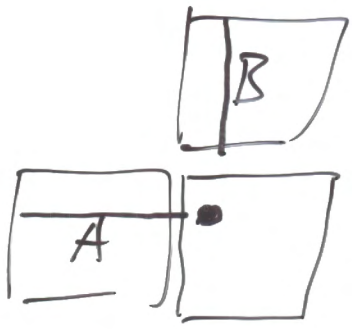
$a \cdot (b+c) = a \cdot b + a \cdot c.$

$\oplus N^1 T$: $0 \neq 1.$

This means: $\mathbb{F}_2$ is a field.

Brico
7.10.14
(5)

Matrix multiplication:



• = sum of coordinatewise product of — with |.

eg:

$$M \cdot x = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$x_0\ x_1\ x_2\ x_3$

To solve the game now simply solve the linear equation

$$e' = e + Mx$$

by the Gauß-Jordan algorithm.

Exercise

Solve 1.1 (i) with this approach.

Solution

$$\begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} \cdot & 0 & \cdot \\ \cdot & \cdot & 0 \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix} \cdot x$$

bricO
7.10.14
(7)

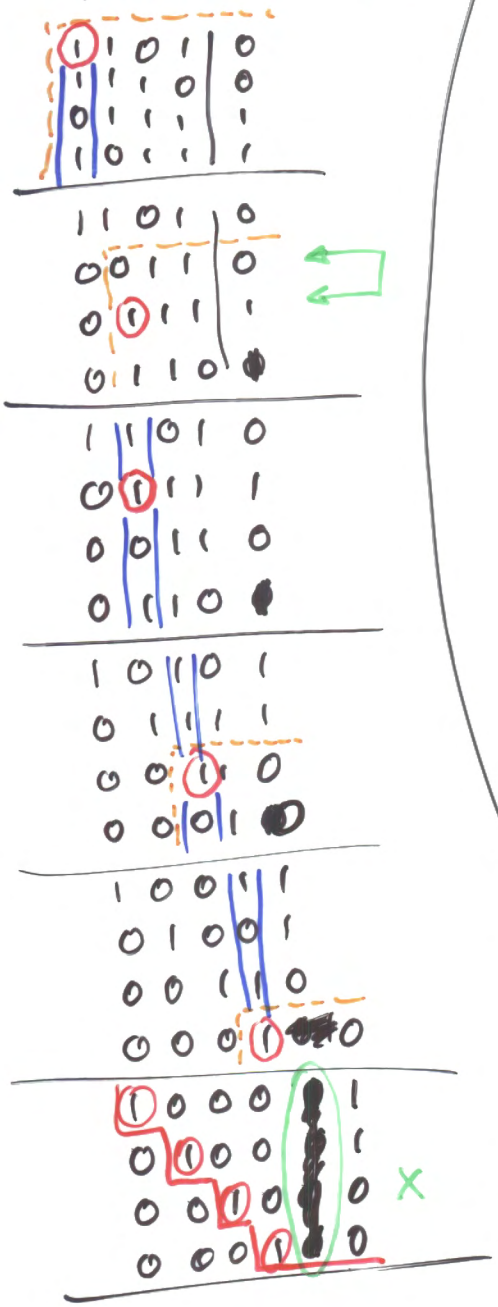
i.e.

$$\begin{bmatrix} \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \end{bmatrix} x = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \end{bmatrix}$$

Gauß-Jordan-Algorithm

Repeat until remaining area is empty.

Gauß-Jordan-algorithm



① Find a new Pivot element in the area below, right of the previous one. Proceed from top-left column by column.

② Swap rows, namely the top remaining row and the one containing the Pivot element if necessary.

③ Scale the row with the Pivot element so that the Pivot becomes 1.

④ Add a multiple of the Pivot row to each other row in order to clear out the rest of the Pivot column.

$\Leftrightarrow$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot x = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$= x$

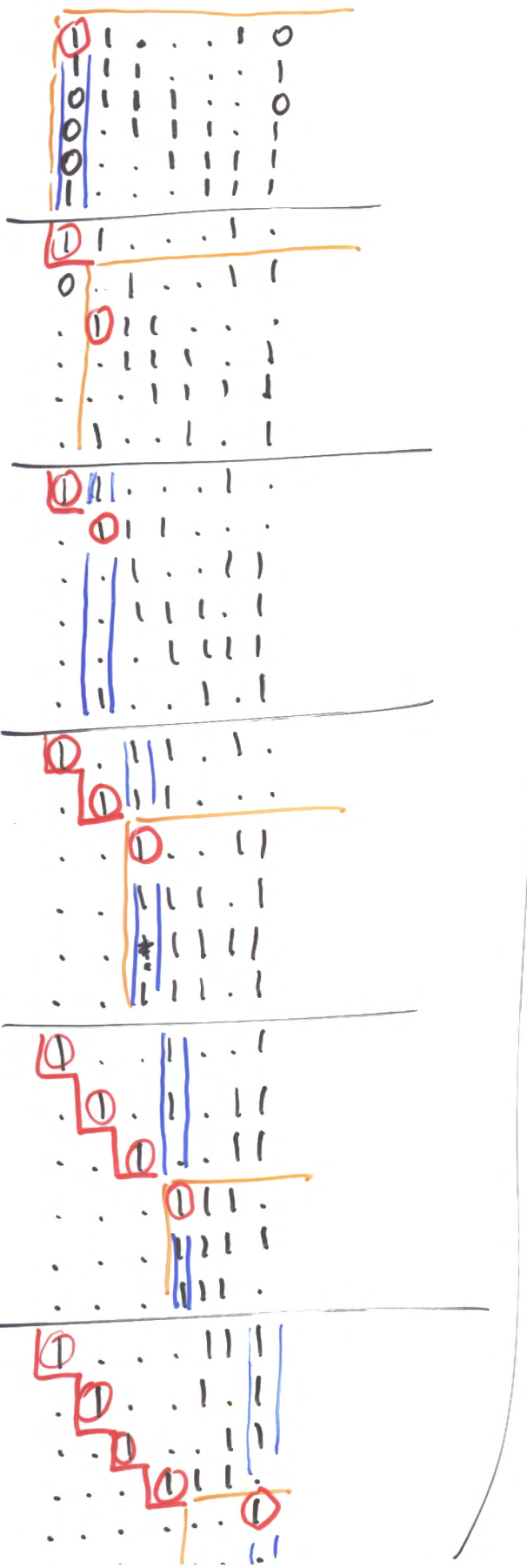
Test solution: $M \cdot x = M \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$ ✓

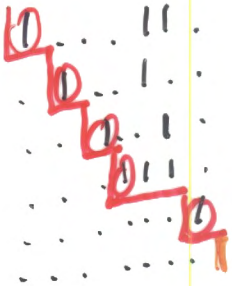
1.1 (ii)

bico
7.10.14

$$\begin{bmatrix} \\ \\ \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{bmatrix} \cdot x$$

Running Gauß-Jordan gives:





But this means:

$$\underbrace{0x_0 + \dots + 0x_5}_{=0} = 1$$

false

So no solution exists!

Runtimes:

- First brute force:
  unlimited tree → infinite (unbounded)

- Second brute force:
  tree without repetitions: $\Omega(n!\cdot n)$ bitop's

  $< O(n^n)$

  $= e^{n \ln n}$

  worse than exponential.

- Third: via Gauß-Jordan:

$$O(n^3)$$

Strassen (1969)

with only 7 multiplications instead of 8 and without changing order.

$\hookrightarrow O(n^{\log_2 7})$

≈ 2.83

record: $O(n^{2.38})$

Another example for Gauß-Jordan-Algo:

brico
8.10.14
1

$$\underbrace{\begin{bmatrix} 0 & 1 & 2 & -1 & 0 & -1 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{=:A} x = \underbrace{\begin{bmatrix} -3 \\ 3 \\ -1 \\ 0 \end{bmatrix}}_{=:b} \quad \text{over } \mathbb{F}_7 = \mathbb{Z}_7$$

where $\mathbb{F}_7 = (\{-3,-2,-1,0,1,2,3\}, +, \cdot)$

$$a+b := [\mathbb{F}_7]((a +_{\mathbb{Z}} b) \bmod 7),$$

where: For $u, v \in \mathbb{Z}$, $v \neq 0$, $u \bmod v$ is defined via division with remainder:
Write
$$u = q \cdot v + r$$
with
$$q, r \in \mathbb{Z}, \quad -\frac{|v|}{2} \leq r < \frac{|v|}{2}$$
Then put $u \bmod v := r$.

$$a \cdot b := [\mathbb{F}_7]((a \cdot_{\mathbb{Z}} b) \bmod 7).$$

Solution

$$\begin{array}{cccccccccc} 0 & 1 & 2 & -1 & 0 & -1 & 1 & 0 & 3 & -3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

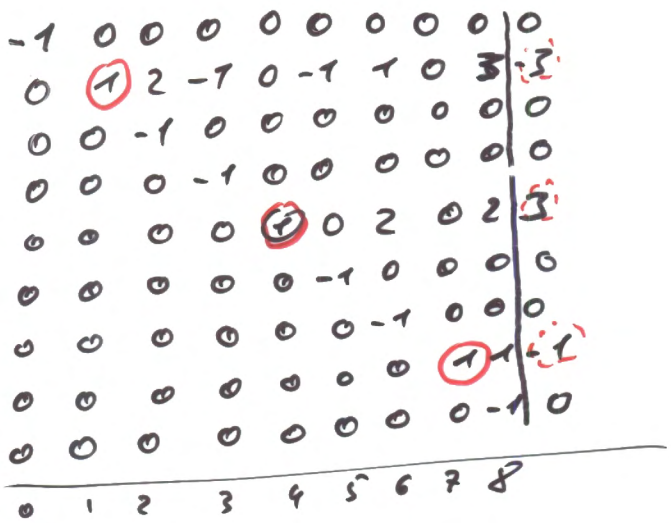
This is called (strong) row-echelon-form.

The Gauß-Jordan-Algorithm always ends with a matrix in (strong) row-echelon-form.

Next, execute expansion

if there is no line ⚠ "0 = 1" as that would mean "no solution".

Produce a matrix with +1 or −1 on the diagonal. If a column has a Pivot element, take that row. Otherwise, add − unit vector



Now, ... by a miracle ... the solution is:

$$\{ x \in \mathbb{F}_7^9 \mid Ax = b \} = \left\{ \begin{bmatrix} 0 \\ -3 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} + \alpha_0 \begin{bmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 2 \\ -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 0 \\ -1 \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_5 \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_6 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha_8 \begin{bmatrix} 0 \\ 3 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} ; \right.$$

$$\left. \alpha_0, \alpha_2, \alpha_3, \alpha_5, \alpha_6, \alpha_8 \in \mathbb{F}_7 \right\}.$$

△

We check: $A \begin{bmatrix} 0 \\ -3 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} = b$, $A \begin{bmatrix} 0 \\ 2 \\ -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $A \begin{bmatrix} 0 \\ 3 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

Actually, we always have $A x_{special} = b$

and $A x_i = 0$ if i is not Pivot,

where $\left[x_0, \ldots, x_{n-1} \mid x_{special} \right]$ is the row-echelon form of $[A|b]$.

expanded

Thus*

$$A\left(x_{special} + \sum_{i \text{ non-Pivot}} \alpha_i x_i\right) = b$$

* Here we use that matrix multiplication is linear:

$$A \cdot (x+y) = A \cdot x + A \cdot y$$

$$A \cdot (\alpha x) = \alpha \cdot (A \cdot x)$$

Proof: That is all true .... ! (Believe me! Or... better... prove it!) □

A vector space V over a field F is...

an oo-class
with a set of elements V
and operations $+ : V \times V \to V$
$\alpha\cdot : F \times V \to V$

and PANIC$^+$, PAND$^{\cdot +}$,

Simplest examples are $V = (F^n, +, \alpha\cdot)$ where $n \in \mathbb{N}$.

"Essentially", these are all "finite-dimensional" [i.e. small] vector spaces.

Example

Consider $V := \{ \mathbb{F}_2^5 \longrightarrow \mathbb{F}_2 \}$

description 1 ~~tab~~ a map as a table

x_0 ..... x_4	$f(x_0, \dots x_4)$
0 0	$f(0, \dots, 0)$

} 2^5 rows with two options each.

So $V \simeq \mathbb{F}_2^{2^5} = \mathbb{F}_2^{32}$

description 2 a map as a polynomial.

Actually, each f can be uniquely written as a polynomial with degree at most one in each variable.

That is:

$$f(x_0, \dots, x_4) = \sum_{I \subset \{0, \dots, 4\}} f_I \cdot \prod_{i \in I} x_i$$

write down / store the vector $(f_I)_{I \subset \{0,\dots,4\}}$

$f_I \in \mathbb{F}_2$; 32 indices

So again $V \simeq \mathbb{F}_2^{2^5} = \mathbb{F}_2^{32}$.

Fact Every vector space V has a basis B.

That is a set B such that every element of V can be written uniquely as a finite combination of elements in B: $\forall x \in V \; \exists \alpha \in F^B$:

$$x = \sum_{b \in B} \alpha_b \cdot b$$

with only finitely many non-zero summands.

Theorem: The length of any basis of V is the same.

Call it <u>dimension of V</u>.

A matrix A describes a 'nice' map

$$f : V \longrightarrow W$$

where 'nice' = linear, ie. $f(v+w) = f(v) + f(w)$,

$$f(\alpha \cdot v) = \alpha \cdot f(v).$$

Next: given a matrix we define $A \in F^{m \times n}$

$$\ker A = \{ x \in F^n \mid Ax = 0 \}$$

and

$$\operatorname{im} A = \{ Ax \in F^m \mid x \in F^n \}.$$

Example

$$\mathbb{F}_4 := \mathbb{F}_2[x] / \langle x^2+x+1 \rangle$$

$$= \{ 0, 1, x, x+1 \}$$

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$\mathbb{F}_4$ is (1) a field,

(2) a vector space over $\mathbb{F}_2$ (of dim 2).

Consider the "Frobenius map":

$$\varphi: \begin{array}{ccc} \mathbb{F}_4 & \longrightarrow & \mathbb{F}_4 \\ a & \longmapsto & a^2 \end{array}$$

It is $\mathbb{F}_2$-linear! Freshman's dream

$$\varphi(a+b) = (a+b)^2 = a^2 + b^2 = \varphi(a) + \varphi(b).$$

Thus we could describe φ as a matrix!

LESSON: Not every linear map comes with a matrix...

Theorem Let $A \in F^{m \times n}$ (i.e. $A : F^n \to F^m$).
Then $\dim \ker A + \dim \operatorname{im} A = n$.
↑
# of columns of A.

Proof

Note that this makes sense!
- Since $\ker A$ and $\operatorname{im} A$ are indeed vector spaces.

$\ker A$: $+ : \ker A \times \ker A \to \ker A$, $(x, y) \mapsto x+y$?

We know $Ax=0$, $Ay=0$. So $A(x+y) = Ax + Ay = 0+0 = 0$.
↑
A linear

$\cdot : F \times \ker A \to \ker A$, $(\alpha, x) \mapsto \alpha \cdot x$?

We do know $Ax=0$. So $A \cdot (\alpha x) = \alpha \cdot Ax = \alpha \cdot 0 = 0$
↑
A linear

Proof (Theorem):

By the Gauß-Jordan-Algorithm + explanation we know:

$\dim \ker A = n - \#\text{Pivots}$

$\dim \operatorname{im} A = \#\text{Pivots}$

(since $\operatorname{im} A$ has those columns of A as a basis which correspond to the Pivots in the row-echelon-form).

□

Example Solve

$$\begin{bmatrix} -1 & -2 & 0 & 3 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & -1 \end{bmatrix} x = \begin{bmatrix} 0 \\ 3 \\ 1 \end{bmatrix}$$ over $\mathbb{F}_7$.

bricolage 8.10.14 (8)

Hint:

a	1	2	3
$\frac{1}{a} = a^{-1}$	1	-3	-2

Solution We use Gauß-Jordan-Algorithm:

$$\left[\begin{array}{|c|cccc} \boxed{-1} & -2 & 0 & 3 & 0 \\ 2 & 0 & 1 & 0 & 3 \\ 0 & 0 & 2 & -1 & 1 \end{array}\right] \quad / \cdot (-1) \qquad =: B$$

Question: $\det B$?

Answer: 1.

$$\left[\begin{array}{cc|ccc} 1 & 2 & 0 & -3 & 0 \\ 0 & \boxed{3} & 1 & -1 & 3 \\ 0 & 0 & 2 & -1 & 1 \end{array}\right] \quad / \cdot \tfrac{1}{3} \equiv \cdot (-2)$$

$$\left[\begin{array}{ccc|cc} 1 & 0 & -3 & 0 & -2 \\ 0 & 1 & -2 & 2 & 1 \\ 0 & 0 & \boxed{2} & -1 & 1 \end{array}\right] \quad / \cdot (-3)$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3 & -3 \end{array}\right]$$

Now expand:

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right]$$

Voting:

0	2, IIII = 7
1	3+1, IIII IIII = 14
2	0, III = 3
3	0, II = 2
-3	3 = 0
-2	1 = 1
-1	II = 3

So the set of solutions is

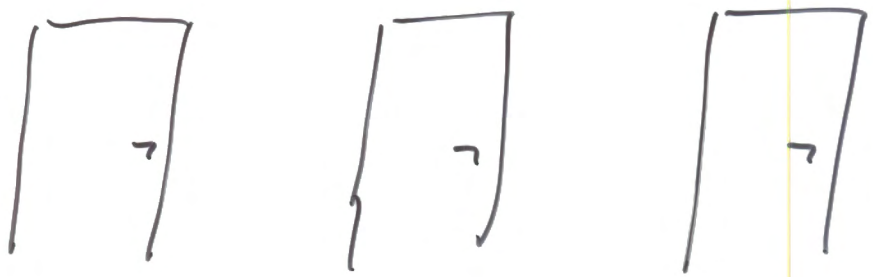
$$\begin{bmatrix} 3 \\ 2 \\ -3 \\ 0 \end{bmatrix} + \mathbb{F}_7 \cdot \begin{bmatrix} 2 \\ 1 \\ 3 \\ -1 \end{bmatrix}.$$

Here: $\dim \ker A = 1$, $\dim \operatorname{im} A = 3$ $\Big\}$ $+ = 4$ ✓

Spoiler on probabilities

brico
8.10.14
(9)

The Monty Hall Problem



- one big prize, two goats.
- Monty Hall let's the candidate choose one door.
- Monty Hall then opens one of the other doors and reveals a goat.
- Monty Hall allows the candidate to switch to the remaining door if she wants

Question: Should she switch or not?

Back to our game (Ex 1.1):

Theorem

Consider the game with n lamps.

Then:

(i) If $n \not\equiv_3 0$ (i.e. $3 \nmid n$)

then there is always a unique solution.

(ii) If $n \equiv_3 0$ (i.e. $3 \mid n$)

then a quarter of the cases has four solutions,

the remaining three quarters have no solution..

Note: for $n=4$ the row-echelon form of M is the unit matrix, and this proves that case.

for $n=6$ the row-echelon form of M is $\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 0 \end{bmatrix}$, and this proves $\dim \ker M = 2$, and so settles this case.

About the proof: consider

$$M = \underbrace{\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 1 \\ 1 & & & & & 0 \\ 0 & & & & & \vdots \\ \vdots & & & & & 0 \\ 0 & & & & & 1 \\ 1 & 0 & \cdots & & 0 & 1 \end{bmatrix}}_{n} \Big\} n$$

Clearly, operating all switches changes all lights!

$$M \cdot \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}.$$

operating every third switch changes all lights $\pmod 3$

$$M \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ \vdots \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}.$$

Thus:

$$M \cdot \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}.$$

Similarly, $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ \vdots \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \end{bmatrix} \in \ker M.$

Finally:

$$\ker M \supseteq \left\{ 0, \begin{bmatrix} 0 \\ 1 \\ 1 \\ \vdots \\ \vdots \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ \vdots \\ \vdots \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ \vdots \end{bmatrix} \right\}.$$

And cutting off the first and last column of M gives

$$'M = \begin{bmatrix} 1 & & & \\ 1 & 1 & & \\ 1 & 1 & \ddots & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix} \quad \begin{matrix} \Rightarrow \\ \Rightarrow \end{matrix} \quad \left.\begin{matrix} x_0 = 0 \\ x_1 = 0 \end{matrix}\right\} \Rightarrow x = 0$$

Claim: $'M \cdot x = 0$ iff $x = 0$. $\square$

Thus $\dim \ker M \geq 2$,

$\dim \operatorname{im} M \geq n-2$.

⌜The claim shows $\dim \ker {}'M = 0$.

So $\dim \operatorname{im} {}'M = n-2$.

Thus $\dim \operatorname{im} M \geq n-2$. ⌟

Since $\dim \ker M + \dim \operatorname{im} M = n$,

both inequalities must be equations: $\boxed{\dim \ker M = 2}$.

This settles (ii) of the previous Theorem.

Determinants

Def Let $A \in F^{n \times n}$ square matrix.

Then we define the determinant

$$\det A = \sum_{\pi \in S_n} (-1)^{\operatorname{sgn}(\pi)} \prod_{i<n} A_{i,\pi(i)}$$

S_n ↑ permutation of $[0,\dots,n-1]$. (ie. $\pi : \{0,\dots,n-1\} \circlearrowleft$ bijective).

where $\operatorname{sgn} \pi$ = # swaps needed to sort the list $[\pi(0),\dots,\pi(n-1)]$

rem 2.

↑ Same as mod, but $\in \mathbb{Z}$.

Note An algorithm derived from this formula has runtime $\Omega(n! \cdot n)$ operations in F. This is VERY slow. ($n! \cdot n \geq n^n = e^{n \ln n}$).

Properties

- $\det A$ invertible (non-zero) $\iff$ A invertible. [ie. $\exists B : A \cdot B = \mathbb{1}$, $B \cdot A = \mathbb{1}$.]
- $\det(AB) = \det A \cdot \det B$,
  $\det \mathbb{1} = 1$.

- if $\tilde{A}$ is the matrix A with the rows k, ℓ swapped
  then $\boxed{\det \tilde{A} = -\det A.}$

- if C is the matrix A with row k scaled by the constant α
  then $\boxed{\det C = \alpha \cdot \det A}$

- if C is the matrix A with row k replaced by row k plus a multiple of row ℓ, $\ell \neq k$,
  then $\boxed{\det C = \det A}$

Thus the Gauß-Jordan-Algorithm can be used to compute the determinant in time $O(n^3)$:

For every row swapping multiply a register by -1.
For every newly found Pivot element multiply by it.
If the final result is the unit/identity matrix
then the register will give the determinant.
Otherwise the determinant is zero.

Inverse matrix, how to compute it?

Run the Gauß-Jordan-Algo on $\boxed{A \mid \mathbb{1}}$ and obtain $\mathbb{1} \mid B$.
Then $B \cdot A = \mathbb{1}$ and so also $A \cdot B = \mathbb{1}$.

Foundations of informatics — a bridging course
Fall 2014
Mathematical tools
MICHAEL NÜSKEN

2. A network problem

Consider a streaming application over the bufferless network in Figure 2.1. We want to transmit a movie through the network from b-it to you. The numbers at the edges indicate how many MBit/sec may be transported over that connection. In order to do that the film is split into small packets. Note that a larger bandwidth can also be used to lower the average time for transmitting a packet over it. There are two important aspects:

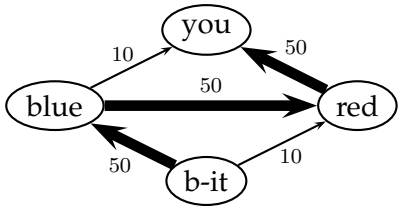


Figure 2.1: Network

(V) The data sent out from a node must always be equal (and not less) to the data received. Otherwise, data would pile up at a node. For example, $f_{\text{b-it,blue}} = f_{\text{blue,red}} + f_{\text{blue,you}}$, where $f_{x,y}$ denotes the flow from node x to node y, that is, the number of packets transmitted. (Note that there is a flow f 'into' the node b-it and a corresponding flow f out of the node you.)

(E) The time a specific packet needs must be almost constant regardless of its path through the network. Otherwise, the recipient machine would have too much work in reassembling the packets in the original order. (We assume that a little buffer space is available to smooth over variations in the network.) For example, $t_{\text{b-it,blue}} + t_{\text{blue,you}} = \text{totaltime}$, where $t_{x,y}$ is the time needed to transmit one packet from x to y. The total time must be the same for all connections.

This is very similar to an electronic current.

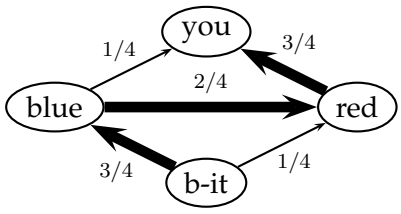


Figure 2.2: Relative flows

Exercise 2.1. (10 points)

(i) Set up a system of linear equations describing the entire system. [4]

(ii) Solve it and read off the flows. [4]

(iii) Determine the complete flow f. [2]

As a control of your results the resulting relative flows are given by Figure 2.2.

Foundations of informatics — a bridging course
Fall 2014
Mathematical tools
MICHAEL NÜSKEN

3. Probabilities

Exercise 3.1 (Randomness helps). (12+4 points)

Give examples where randomness

(i) decides about win or loose. 2

(ii) helps simulating difficult reality. 2

(iii) helps solving difficult finite problems. 2

(iv) models errors. 2

(v) makes decisions. 2

(vi) hides secrets. 2

(vii) Does something else which is interesting. +4

Exercise 3.2 (Conference breakfast). (5 points)

You are at a probability theory conference. 60% of the participants are British. 75% of the British eat ham at breakfast, yet only 25% of the others. This morning your table neighbour eats ham. What is the probability that she is British? 5

Exercise 3.3 (Monty Hall Problem). (8 points)

We are guests in a game show and close to win a great fortune. The quiz master asks us to choose one of three (closed) doors. She explains that behind one of them awaits you a million Euros. Once you fixed your choice the quiz mastress opens one of the other doors and shows you that this was only a goat. She gives you a final chance: you may either retain your door or switch to the remaining closed one.

(i) Say door 3 is opened. Calculate the conditional probability that your door is the winning one given that the door 3 is a fail, and its complement. 2

(ii) Calculate the unconditional probability that your door is the winning one, and its complement. 1

What do you do? Reason! 5

Exercise 3.4 (Prisoner's dilemma). (10 points)

A hundred prisoners are given a great opportunity. Some of them may make a day trip to the nearby theatre. Each of them can make one of two choices: either choose to join the trip or not to join the trip. All who want can see the piece, yet only unless all of them choose to go.

The prisoners cannot communicate with each other, all are equally selfish, and follow the same strategy. Strategy 0 is to choose not to go. Then nobody goes. Strategy 1 is to choose to go. Then nobody goes.

8 (i) Find a strategy that allows some of them to go.

2 (ii) Optimize the strategy so that the expected number of prisoners to see the show is larger than 94.5.

Exercise 3.5 (Random exit). (8 points)

You are trapped again in a locked room. Once every hour you have the chance to open the door. This succeeds with a certain probability p.

(i) What is the chance that you can leave the room after

0 (a) exactly one hour?

1 (b) exactly two hours?

1 (c) exactly three hours?

1 (d) exactly four hours?

(ii) What is the expected number of hours that you have to stay

3 (a) ... by definition? [Give a formula.]

2 (b) ... by value? [Calculate!]

A steep intro to finite probabilities

To keep things simple

brico
9.10.14
(1)

1. Events

- A universe Ω is a finite set of possible outcomes of an experiment or a random source.
- An event A is just a subset of Ω, $A \subset \Omega$.
- There is a function "prob" which attributes a probability to each event: $\text{prob} : \{A \mid A \subseteq \Omega\} \to [0,1]$

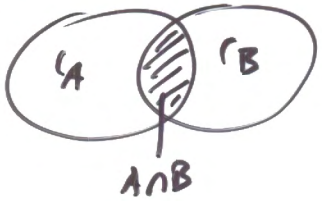
subject:

$$\text{prob}(\emptyset) = 0,$$
$$\text{prob}(A \,\dot\cup\, B) = \text{prob}\, A + \text{prob}\, B$$
$$\text{prob}(\Omega) = 1.$$

(i.e. disjoint union. It means $A \cup B$ and assume $A \cap B = \emptyset$)

Consequence:

- $\text{prob}(\Omega \setminus A) = 1 - \text{prob}\, A.$
- $\text{prob}(A \cup B) = \text{prob}\, A + \text{prob}\, B - \text{prob}(A \cap B).$



$\ulcorner$ $'A := A \setminus B$, $'B = B \setminus A$.

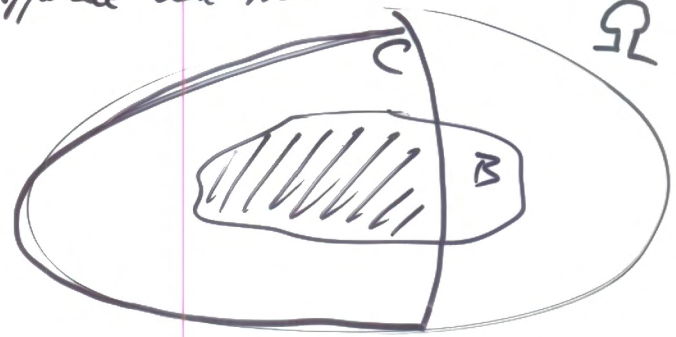
Then $\text{prob}(A \cup B) = \text{prob}('A \,\dot\cup\, B)$
$= \text{prob}('A) + \text{prob}(B),$

$\text{prob}(A) = \text{prob}('A \,\dot\cup\, (A \cap B))$
$= \text{prob}('A) + \text{prob}(A \cap B).$

Take the difference and that's it. $\lrcorner$

Conditional probabilities

Given that C occured what is the probility for landing in B.



$$\text{prob}(B \mid C) := \frac{\text{prob}(B \cap C)}{\text{prob}\, C}$$

Only assumption: $\text{prob}\, C \neq 0$.

Def A and B are <u>independent</u>

iff $\text{prob}(A \cap B) = \text{prob}\, A \cdot \text{prob}\, B$

iff $\text{prob}(A \mid B) = \text{prob}\, A$.

Ex Rolling a die: $\Omega = \{1, 2, 3, 4, 5, 6\}$ with uniform distribution

$C = \{2, 4, 6\}$ $\quad$ $\text{prob}\, B = \frac{1}{2}$, $\neq \text{prob}(B \mid C) = \frac{2}{3}$

$B = \{4, 5, 6\}$ $\quad$ ↳ B, C not independent

$B' = \{5, 6\}$ $\quad$ $\text{prob}\, B' = \frac{1}{3} = \text{prob}(B' \mid C) = \frac{1}{3}$ $\quad$ B', C indep.

2. Random variables (r.v.)

Def A random variable X is a function on the universe Ω:

$$X : \Omega \longrightarrow S.$$

We always assume that we know its "distribution":

$$\begin{aligned} S &\longmapsto [0,1], \\ x &\longmapsto \text{prob}(X = x). \end{aligned}$$

Based on the previous $\text{prob}(X=x) = \text{prob}(\{\omega \in \Omega \mid X(\omega) = x\})$.

Property: $\sum_{x \in S} \text{prob}(X = x) = 1$.

Def Two r.v. X and Y are independent:

$\forall\, x \in \text{range } X,\ y \in \text{range } Y$.

$$\text{prob}(X = x \wedge Y = y) = \text{prob}(X = x) \cdot \text{prob}(Y = y).$$

More generally: n r.v.s $X_0, \ldots, X_{n-1}$ are indep:

$$\text{prob}\Big(\bigwedge_i X_i = x_i\Big) = \prod_i \text{prob}(X_i = x_i)$$

Monty Hall

Two answers! Yes. No. Doesn't matter.

17+1 1+2. 4

Random exit

Consider a program

```
REPEAT
    arbitrary stuff
UNTIL condition C holds
```

with the only property that $\text{prob}(C \text{ holds}) = p \in [0,1]$, and after each execution of the loop, $p \neq 0$.

For a nice solution we introduce r.v.

$$X_i = \begin{cases} 1 & \text{if } C \text{ holds after round } i, \\ 0 & \text{otherwise.} \end{cases}$$

We assume that all (X_i) are independent and $\text{prob}(X_i = 1) = p$.

To keep everything finite, only consider $i < n$ for some fixed (but unspecified) $n \in \mathbb{N}$.

We want to analyze the r.v.

$$N = \#\text{ rounds til exit.}$$

where

$$N = j \iff X_j = 1 \wedge X_{j-1} = 0 \wedge \dots \wedge X_1 = 0$$

Now we can calculate:

$$\begin{aligned} \text{prob}(N=j) &= \text{prob}(X_j = 1 \wedge X_{j-1} = 0 \wedge \dots \wedge X_1 = 0) \\ &\overset{\text{indep}}{=} \text{prob}(X_j = 1) \cdot \text{prob}(X_{j-1} = 0) \cdot \dots \cdot \text{prob}(X_1 = 0) \\ &= p \cdot (1-p) \cdot \dots \cdot (1-p) \\ &= p\,(1-p)^{j-1}. \end{aligned}$$

brico
9.10.14
4

Def The expected value of a ~~(real-valued)~~ r.v. Z with values in $\mathbb{R}$ is defined as

$$E(Z) := \sum_{z \in \text{range } Z} z \cdot \text{prob}(Z = z)$$

For N this means:

$$E(N) = \sum_{1 \le j \le n} j \cdot \text{prob}(N = j) + \text{prob}(\text{"}N > n\text{"})$$

$$= p \cdot \sum_{1 \le j \le n} j \, (1-p)^{j-1} + \underbrace{\underbrace{(1-p)}_{<1}{}^{n}}_{\to 0}$$

$$\xrightarrow{n \to \infty} \underbrace{p \cdot \underbrace{\sum_{1 \le j} j \, (1-p)^{j-1}}_{= \frac{1}{p^2}}}_{} \ldots$$

$$= \frac{1}{p}.$$

We know

$$\sum_{j \ge 0} x^j = \frac{1}{1-x}$$

for $|x| < 1$.

Differentiate by x:

$$\sum_{j \ge 1} j \cdot x^{j-1} = \frac{1}{(1-x)^2}.$$

Ok, due to uniform convergence.

Theorem

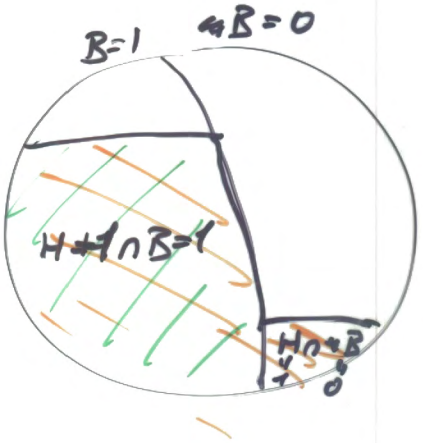
The expected number of iterations of the Loop in the random exit with exit probability $p \neq 0$ is $1/p$.

$\square$

Ex 3.2

$$B = \begin{cases} 1 & \text{if nationality is British,} \\ 0 & \text{otherwise.} \end{cases}$$

$$H = \begin{cases} 1 & \text{if the person eats ham,} \\ 0 & \text{otherwise.} \end{cases}$$



we do know:

$$\text{prob}(B=1) = 0.6 = \tfrac{3}{5}.$$

$$\text{prob}(H=1 \mid B=1) = 0.75 = \tfrac{3}{4}.$$

$$\text{prob}(H=1 \mid B=0) = 0.25 = \tfrac{1}{4}.$$

we want:

$$\text{prob}(B=1 \mid H=1) = ?$$

From our knowledge we find:

H \ B	0	1	
0			
1	2/20	9/20	11/20
	2/5	3/5	1

$$\text{prob}(B=0) = \tfrac{2}{5} = 1 - \tfrac{3}{5}$$

$$\text{prob}(H=1 \wedge B=1) = \text{prob}(B=1) \cdot \text{prob}(H=1 \mid B=1) = \tfrac{3}{4} \cdot \tfrac{3}{5} = \tfrac{9}{20}$$

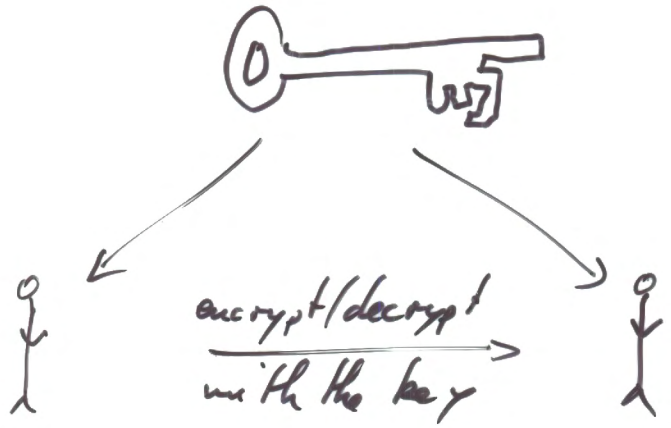
$$\text{prob}(H=1 \wedge B=0) = \text{prob}(B=0) \cdot \text{prob}(H=1 \mid B=0) = \tfrac{2}{5} \cdot \tfrac{1}{4} = \tfrac{2}{20}$$

$$\text{prob}(H=1) = \text{prob}(H=1 \wedge B=1) + \text{prob}(H=1 \wedge B=0) = \tfrac{9}{20} + \tfrac{2}{20} = \tfrac{11}{20}$$

so

$$\text{prob}(B=1 \mid H=1) = \frac{\text{prob}(B=1 \wedge H=1)}{\text{prob}(H=1)} = \frac{9/20}{11/20} = \frac{9}{11} = 81.8\%$$

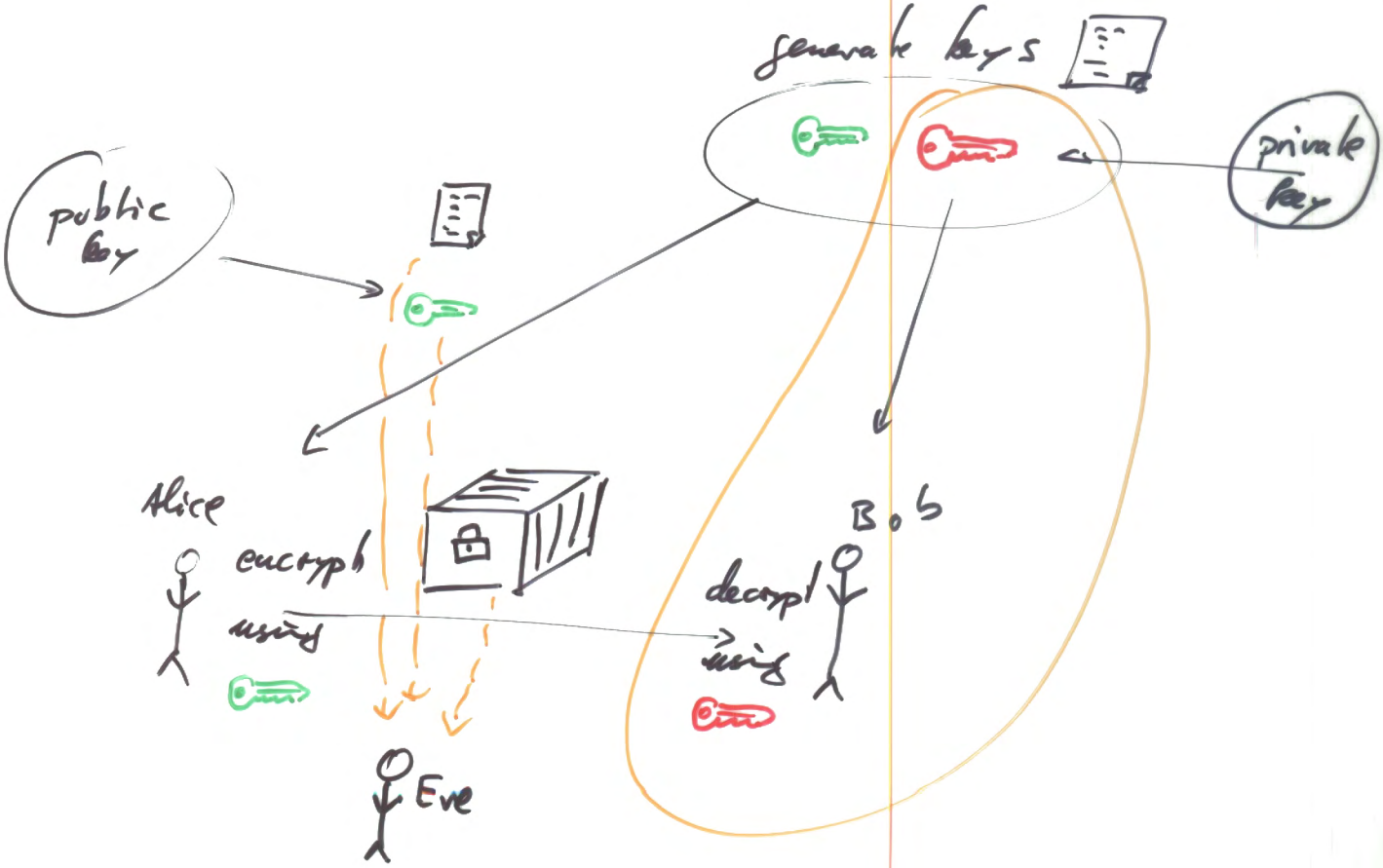
Classical:



New solution: [1970-1972 British Secret Service: Non-secret encryption]

1976 Diffie & Hellman

1978 Rivest, Shamir & Adleman: RSA.



RSA

generate_keys

Input: security parameter $k \in \mathbb{N}$.
Output: a key pair

$O(k^4)$ 1. Generate a random prime p of about $k/2$ bits length.
$O(k^4)$ 2. Generate a random prime q of about $k/2$ bits length.
$O(k^2)$ 3. Compute $N := p \cdot q$.
$O(k^2)$ 4. Compute $L := (p-1) \cdot (q-1)$.
5. Find two numbers $e, d \in \mathbb{Z}$, $0 < e, d < L$ such that
$O(k^4)$
$$e \cdot d = 1 - t \cdot L$$
for some $t \in \mathbb{Z}$.
6. Return public key (N, e) for encryption,
private key (N, d) for decryption.

$O(k^4)$

encrypt

Input: public key (N, e),
message $x \in \{0, \dots, N-1\} = \mathbb{Z}_N$.
Output: ciphertext $y \in \mathbb{Z}_N$.
$O(k^3)$
1. $y = x^e$ in $\mathbb{Z}_N$.
2. Return y.

decrypt

Input: private key (N, d),
ciphertext $y \in \mathbb{Z}_N$.
$O(k^3)$
Output: supposed message $z \in \mathbb{Z}_N$.
1. $z = y^d$ in $\mathbb{Z}_N$.
2. Return z.

brico
9.10.14
(8)

Todo

(0) Understand the program.

(1) Correctness? Is $z = x^r$?

(2) Efficiency? Is everything reasonably fast?

(3) Security?

Easiest first:

Integers modulo N

$$\mathbb{Z}_N := (\{0,1,2,\dots,N-1\}, +, \cdot)$$

($+$: addition, $\cdot$: multiplication modulo N)

$$a + b := (a +_{\mathbb{Z}} b) \bmod N$$
$$= [\mathbb{Z}_N]((a +_{\mathbb{Z}} b) \operatorname{rem} N),$$
$$a \cdot b := (a \cdot_{\mathbb{Z}} b) \bmod N.$$

Implementing this as a C++ class is easy given arithmetic in $\mathbb{Z}$.

Runtime $(+) \in \mathcal{O}(k)$
Runtime $(\cdot) \in \mathcal{O}(k^2)$
— k = bitlength of N.

Karatsuba (1995?): $(x_1 b + x_0) \cdot (y_1 b + y_0)$
$= x_1 y_1 \cdot b^2 + (\underbrace{x_1 y_0 + x_0 y_1}_{(x_1+x_0)\cdot(y_1+y_0) - x_1 y_1 - x_0 y_0}) \cdot b + x_0 y_0$

$\hookrightarrow \mathcal{O}(k^{\log_2 3})$

Schönhage (1971) (FFT) $\mathcal{O}(k \log k \log\log k)$

Fürer (2007?): $\mathcal{O}(k \log k \, 2^{\log^* k})$

The construction is based on the

Theorem (Division with remainder in $\mathbb{Z}$)

Given two integers $x, y \in \mathbb{Z}$, $y \neq 0$,
then there exist (unique) integers $q, r \in \mathbb{Z}$
such that

$$x = q \cdot y + r$$

and $$0 \leq r < |y|.$$

Given x, y we define $x \operatorname{rem} y := r \in \mathbb{Z}$,
$x \operatorname{quo} y := q$,
and $x \bmod y := [\mathbb{Z}_N](r) \in \mathbb{Z}_N$.

Theorem

Given any integer $N \geq 2$ the
$\mathbb{Z}_N$ is a (finite) commutative ring with 1,
i.e. it fulfills PANIC$^+$, PAN C$^\cdot$, D$^{\cdot+}$ØNT.

Proof (partly)

P+: we have to check that for $a, b \in \mathbb{Z}_N$
also $a + b \in \mathbb{Z}_N$.

A$^\cdot$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$?

$$(a \cdot b) \cdot c = [\mathbb{Z}_N][((\underbrace{a \cdot_{\mathbb{Z}} b \operatorname{rem} N}) \cdot_{\mathbb{Z}} c) \operatorname{rem} N]$$

$= a \cdot_{\mathbb{Z}} b - t \cdot_{\mathbb{Z}} N$ for some $t \in \mathbb{Z}$.

$$= [(a \cdot_{\mathbb{Z}} b - t \cdot_{\mathbb{Z}} N) \cdot_{\mathbb{Z}} c] \bmod N \quad \leftarrow D^{\cdot+\mathbb{Z}}$$

$$= [(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c - \underbrace{(t \cdot_{\mathbb{Z}} N) \cdot_{\mathbb{Z}} c}_{(t \cdot_{\mathbb{Z}} c) \cdot_{\mathbb{Z}} N}] \bmod N \quad \leftarrow AC^{\cdot\mathbb{Z}}$$

$$= [(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c] \bmod N \quad \leftarrow A^{\cdot\mathbb{Z}}$$

$$= [a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c)] \bmod N = a \cdot (b \cdot c)$$

bri'co
9.10.14
(10)

FACT: $0 \neq 1$ in $\mathbb{Z}_N$.

because $0 \bmod N \neq 1 \bmod N$

since otherwise $0 + t_1 N = 1 + t_2 N$

$1 - 0 = t \cdot N$,

$1 = t \cdot N$.

Thus $N \mid 1$, i.e. $N = \pm 1$ or $N = -1$.

But $N \geq 2$. □

From now on we may consider the 'class' / ring $\mathbb{Z}_N$ as a black box.

How to compute x^e in $\mathbb{Z}_N$?

Here: $x \in \mathbb{Z}_N$, $e \in \mathbb{N}_{< 2^k}$.

By definition:

$$x^e = \underbrace{(\ldots(((x \cdot x) \cdot x) \cdot x) \ldots) \cdot x}_{e \text{ copies of } x}$$

runtime: $O(e \cdot k^2) \approx O(k^2 \cdot 2^k)$

(Variant: Compute x^e in $\mathbb{Z}$, then reduce mod N.
runtime: $\Omega(e \cdot 2^k) = \Omega(2^{2k})$)

To compute x^8 we would compute $((x^2)^2)^2$,
with 3 instead 7 multiplications.

This brings us to

Repeated Squaring / Square & Multiply

$$\underbrace{x, x^2, x^{2^2}, x^{2^3}, x^{2^4}, \ldots, x^{2^{k-1}}}, \qquad x^e$$

brico
9.10.14
(47)

Since $x^a \cdot x^b = x^{a+b}$ ...

write $e = \sum_{i=0}^{k-1} e_i 2^i$ with $e_i \in \{0,1\}$.

Then

$$x^e = \prod_{\substack{i, \\ e_i \neq 0}} x^{2^i}.$$

Thus we may compute x^e with at most $2(k-1)$ multiplications.

Better (saving memory!)

Algorithm

Input: $x \in \mathbb{Z}_N$, $e \in \{0, \dots, N-1\}$.

Output: $x^e \in \mathbb{Z}_N$.

1. Write $e = \sum_{i=0}^{k-1} e_i 2^i$, $y = 1$.
2. For $j = k-1 \searrow 0$ do
3. $\quad y := y^2 \cdot x^{e_j}$.
4. Return y.

time $O(k^3)$

space $O(k)$

Claim: after step 3 $\quad y = x^{\sum_{i=j}^{k-1} e_i 2^{i-j}}$

for a given j.

Idea: $1 = x^0$, $x^{2 \cdot 0 + e_{k-1}} = x^{e_{k-1}}$,

$x^{2e_{k-1} + e_{k-2}}$,

$x^{4e_{k-1} + 2e_{k-2} + e_{k-3}}$

$\vdots$

x^e

Cool:
runtime: $O(2(k-1))$ multipl.
space: constant.

Example

$e = 27 = 11011_2$

x^0

x^1

$x^{11} = (x^1)^2 \cdot x$

$x^{110} = (x^{11})^2$

x^{1101}

x^{11011}

Next question: How to perform step 5 of generate_keys?

How to find e, d such that

$$e \cdot d + t \cdot L = 1$$

with $e, d \in \{1, \dots, L-1\}$, $t \in \mathbb{Z}$.

Zeroth try:

REPEAT
  Pick $e, d \in_R \{1, \dots L-1\}$
  and compute $r = ed \bmod L$.
UNTIL $r = 1$.

runtime: expected $O(L \cdot \dots) = O(2^k \dots)$

Other try: (Abdallah)

REPEAT
  Pick $e \in_R \{1, \dots, L-1\}$.
  Try to compute $d, t \in \mathbb{Z}$ such
  that $d \cdot e + t \cdot L = 1$. (*)
UNTIL successful

We are left with determining a solution for (*).

Observe that 1 is a very small positive integer.

Let's try to start with an easier task:

Find numbers $s, t \in \mathbb{Z}$
such that
$$s \cdot e + t \cdot L$$
is small.

— and improve stepwise!

brico
9.10.14
(17)

So what are the easiest starting pairs?

s	t	$s \cdot e + t \cdot L =: r$
0	1	L
1	0	e
L	$-e$	0 ← too small!

How can we improve?
→ We can add/subtract equations of the $r = s \cdot e + t \cdot L$!

Let's do an example:

$L = 60$ [$= (7-1) \cdot (11-1)$],

$e = 13$.

r	q	s	t	comment
60		0	1	$60 = 0 \cdot e + 1 \cdot L$
13	4	1	0	$13 = 1 \cdot e + 0 \cdot L$
8	1	-4	1	$8 = -4 \cdot e + 1 \cdot L$ ← $60 - 4 \cdot 13$
5	1	5	-1	$5 = 5 \cdot e + -1 \cdot L$ ← $13 - 1 \cdot 8$
3	1	-9	2	$3 = -9 \cdot e + 2L$ ← $8 - 1 \cdot 5$
2	1	14	-3	
1	2	-23	5	→ $1 = -23 \cdot e + 5L$
0		60	-13	

→ $0 = 60 \cdot e - 13 \cdot L$
trivially true.
Can serve as a crosscheck!

Extended Euclidean Algorithm

EEA

Input: two values a, b

Output: r, s, t

1. $r_0 := a$, $s_0 := 1$, $t_0 := 0$. // $a = 1 \cdot a + 0 \cdot b$
2. $r_1 := b$, $s_1 := 0$, $t_1 := 1$. // $b = 0 \cdot a + 1 \cdot b$
3. $i := 1$.
4. While $r_i \neq 0$ do
5. $\quad q_i := r_{i-1}$ quo r_i, } // $r_{i-1} = q_i \cdot r_i + r_{i+1}$
6. $\quad r_{i+1} := r_{i-1} - q_i r_i$,
7. $\quad s_{i+1} := s_{i-1} - q_i s_i$
8. $\quad t_{i+1} := t_{i-1} - q_i t_i$
9. $\quad$ increment i.
10. $e := i - 1$.
11. Return (r_e, s_e, t_e).

Exercises

Run the EEA for starting numbers

(i) 45, 23

(ii) 11, 57

(iii) 93, 39

(i)

	r	q	s	t
0:	45		1	0
1:	23	1	0	1
2:	22	1	1	-1
3:	1	22	-1	2
4:	0		23	-45

X check: $0 = 23 \cdot a - 45 \cdot b$ ($a = 45$, $b = 23$).

(for each line $r = sa + tb$!)

This is trivially ok.

Result: $(1, -1, 2)$:

$1 = -1 \cdot a + 2 \cdot b$.

$e = 3$.

(ii)

r	q	s	t
11		1	0
57	0	0	1
11	5	1	0
2	5	-5	1
1	2	26	-5
0		-57	11

X check: $0 = -57 \cdot a + 11 \cdot b$ ($a = 11$, $b = 57$) ✓

Thus: $(1, 26, -5)$,

$1 = 26 \cdot a - 5 \cdot b$.

(iii)

r	q	s	t
93		1	0
39	2	0	1
15	2	1	-2
9	1	-2	5
6	1	3	-7
3	2	-5	12
0		13	-31

X check: $0 = 13 \cdot a - 31 \cdot b$ ($a = 93$, $b = 39$)

Not as easy, but ✓

Thus: $(3, -5, 12)$, i.e.

$3 = -5 \cdot a + 12 \cdot b$.

Fact For all i we have

- $r_i = s_i a + t_i b$
- $r_{i-1} = q_i r_i + r_{i+1}$
- $0 \le r_{i+1} < |r_i|$

} division with remainder

Lemma For $i \ge 3$: $|r_{i+1}| \le \frac{1}{2} |r_{i-1}|$

Proof (Ex).

Corollary $\ell \le 2 \max\{ \lceil \log_2 |a| \rceil , \lceil \log_2 |b| \rceil \} + 1.$

ie. runtime (EEA | $\mathbb{Z}$) $\in \mathcal{O}(k^3)$

Pf $1 \le |r_\ell| \le \frac{1}{2^{\lfloor \ell/2 \rfloor - 1}} \underbrace{|r_\ell - 2(\lfloor \ell/2 \rfloor - 1)|}_{\le \max\{|a|, |b|\}}$.

ie.

$$2^{\lfloor \ell/2 \rfloor} \le 2 \max\{|a|, |b|\}.$$

$$\lfloor \ell/2 \rfloor \le 1 + \log_2 \max\{|a|, |b|\}.$$

□

Actually, runtime $\in \mathcal{O}(k^2)$

Def Given two number a, b (the) a greatest common divisor d is a number such that

(i) $d \mid a \wedge d \mid b$,

(ii) $\forall c: \; c \mid a \wedge c \mid b \Rightarrow c \mid d$.

Theorem wiki: $d = \gcd(a,b)$. in abuse of notation!

Fact

(i) $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$,

(ii) $\gcd(a, b) = \gcd(r_\ell, 0) = r_\ell$.

Proof (Fact)

(i) we know $r_{i-1} = q_i r_i + r_{i+1}$.

So if $c \mid r_{i-1}$ and $c \mid r_i$

then $c \mid (r_{i-1} - q_i r_i) = r_{i+1}$.

And vice versa: if $c \mid r_i$ and $c \mid r_{i+1}$

then $c \mid q_i r_i + r_{i+1} = r_{i-1}$.

So (r_{i-1}, r_i) and (r_i, r_{i+1})

have the same set of common divisors,

in particular, their gcds are equal.

(ii) follows from (i) by induction... □

Theorem

The EEA computes in time $O(k^3)$
for two input k-bit numbers a, b
their greatest common divisor r_e
and two numbers s_e, t_e such that

$$r_e = s_e \cdot a + t_e \cdot b \quad \text{[Bézout equation]}$$

r_e = "gcd(a,b)"

Corollary

If the EEA finds $r_e \neq \pm 1$.
then the equation $sa + tb = 1$
has no solution.

Proof r_e is a common divisor of a and b.

Thus $r_e \mid sa + tb \overset{\text{assumed}}{=} 1$ ↯. □

In our very first example for the EEA we obtained:

$$1 = -23 \cdot e + 5 \cdot L$$

So we have the solution $d = -23$, $t = 5$.

But we wanted $0 < d < L = 60$. :-

Notice that we have also

$$0 = 60 \cdot e - 13 \cdot L.$$

Adding gives:

$$1 = 37 \cdot e - 8 \cdot L.$$

This gives the solution $d = 37$, $t = -8$.

Alternatively, think in $\mathbb{Z}_L$:

$$1 = -23 \cdot e + 5 \cdot L$$

means

$$1 = -23 \cdot e \quad \text{in } \mathbb{Z}_{60} = \mathbb{Z}_L.$$

And $-23 = 37$ in $\mathbb{Z}_{60}$.

So $1 = \underbrace{37}_{d} \cdot e$ in $\mathbb{Z}_{60}$.

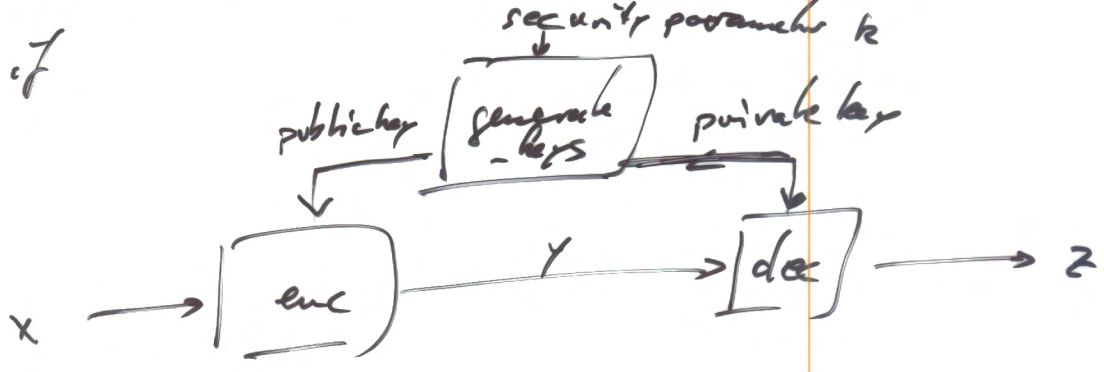
Remark: $L = 60$, $e = 9$ will not produce a solution since $\gcd(L, e) = 3 \neq 1$.

We can find e, d in RSA generate keys in time $O(k^4)$.

bnco
10.10.14
(6)

What about CORRECTNESS?

First what does that mean? Well, we want that if



then $z = x$.

What is z? Well:

$$z = y^d = (x^e)^d = x^{e \cdot d} \quad \text{in } \mathbb{Z}_N$$

by construction of $e \cdot d$:

$$z = x^{1 - t \cdot L} = x \cdot (x^L)^{-t} \quad \text{in } \mathbb{Z}_N.$$

So if $x^L = 1$ we are done...

This cannot always hold: $0^L = 0 \neq 1$,

but fortunately such cases are rare...

and even then $z = x$.

This is a consequence of LAGRANGE's theorem or EULER's theorem or a bit more than FERMAT's little theorem.

Play example

$N = 15 = 3 \cdot 5$

$\mathbb{Z}_N$ $\ni x$	0	± 1	± 2	± 3	± 4	± 5	± 6	± 7
x^{-1}	–	± 1	∓ 7	–	± 4	–	–	∓ 2

Strange: $3 \cdot 5 = 0$. Thus $3 \cdot x \neq 1$ and $5 \cdot x \neq 1$.

「Because otherwise:

$5 = 5 \cdot 1 \overset{\text{!}}{=} 5 \cdot 3 \cdot x = 0 \cdot x = 0$ ↯」

Also $6 \cdot 5 = 0$. So $6 \cdot x \neq 1$.

So there are only 8 elements in $\mathbb{Z}_{15}$ that have inverses.

Observe: $L = (3-1) \cdot (5-1) = 8$. ☺

Side observation: $\mathbb{Z}_{15}$ is not a field.

Let's consider the set $\mathbb{Z}_N^\times$ of invertible elements and keep multiplication with it: $(\mathbb{Z}_N^\times, \cdot)$

Question: Is $(\mathbb{Z}_N^\times, \cdot)$ a commutative group?

P: Is, given x, y invertible, the product $x \cdot y$ also invertible?

Yes: $(y^{-1}x^{-1})(x \cdot y) = y^{-1} \cdot y = 1$.

A: ✓
N: 1 is invertible. ✓
I: Yes, because the inverse of an invertible element is invertible.
C: ✓

brico
10.10.14
(8)

Powers revisited: in $\mathbb{Z}_N^\times$, $N = 15$.

Powers of 2:

k	0	1	2	3	4	5	6	7	8
2^k	1	2	4	−7	−1	−2	−4	7	1

Coincidence: $\# \mathbb{Z}_N^\times = 8$ and $2^8 = 1$.

Hm...?

Powers of 7:

7^k	1	7	4	−2	−1	−7	−4	2	1

again: $7^8 = 1$

Powers of 3:

$$3^8 = (-6)^4 = (6)^2 = 6 \qquad \text{Oops.}$$

But: $3 \notin \mathbb{Z}_N^\times$!

However:

$$3 \cdot 3^8 = 3 \cdot 6 = 3.$$

Theorem (Lagrange)

Given a finite group G.
Then for every element $x \in G$
we have

$$x^{\#G} = 1$$

Proof in case G is commutative:

List G:

$$x_1, x_2, x_3, \ldots, x_\ell$$

where $\ell = \#G$

Multiply by x:

$$x \cdot x_1, x \cdot x_2, x \cdot x_3, \ldots, x \cdot x_\ell.$$

We have:

1. this is again list of elements in G.
2. No element occurs twice.

   ⌜ Otherwise: $x \cdot x_i = x \cdot x_j$
   Multiply by x^{-1} and use associativity and N, I:

   $$x^{-1}(xx_i) = x_i = x_j$$

   But then $i = j$. ⌟

3. None missing.

   ⌜ Say you look for x_i.
   Then $x^{-1}x_i = x_j$ for some j because the first list is complete.
   But then: $x \cdot x_j = x(x^{-1}x_i) = x_i$. ⌟

Thus multiplying each list we obtain (using C!):

brico 10.10.14 (10)

$$x_1 \cdot x_2 \cdot \ldots \cdot x_\ell = x\cdot x_1 \cdot x\cdot x_2 \cdot \ldots \cdot x\cdot x_\ell .$$

But now, dividing by each x_i, we get (using C!):

$$1 = \underbrace{x \cdot x \cdot \ldots \cdot x}_{\ell \text{ times}} = x^\ell = x$$ #6.

□

Theorem (EULER)

Take $G = \mathbb{Z}_N^\times$. Then for any $x \in G$, we have $x^{\varphi(N)} = 1$ in $\mathbb{Z}_N$ where $\varphi(N) := \#\mathbb{Z}_N^\times$ (EULER totient function).

Pf: Use Lagrange's theorem for G. □

Little Theorem (FERMAT)

Let p be a prime, $x \in \mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$

Then $x^{p-1} = 1$ in $\mathbb{Z}_p$

Proof Use Lagrange for $G = \mathbb{Z}_p^\times$ or EULER for $N = p$. □

This actually settles a large part of what we wanted:

for $x \in \mathbb{Z}_N^\times$ we have $x^{\varphi(N)} = 1$ in $\mathbb{Z}_N^\times$.

It remains to show that

$$\varphi(N) = L$$

in our situation $N = p \cdot q$. And that $\frac{\#\mathbb{Z}_N^\times}{\#\mathbb{Z}_N} \approx 1$.

What is $\varphi(p \cdot q)$?

Which elements of $\mathbb{Z}_{pq}$ are <u>not</u> invertible?

Actually, we have:

$$\mathbb{Z}_N^\times = \{ x \in \mathbb{Z}_N \mid x \text{ invertible} \}$$
$$= \{ x \in \mathbb{Z}_N \mid \text{EEA}(x, N) \text{ finds an inverse} \}$$
$$\overset{(3)}{=} \{ x \in \mathbb{Z}_N \mid \gcd(x, N) = 1 \}$$

How to find an inverse? Given $x \in \mathbb{Z}_N$.

Invertible means: $\exists\, s \in \mathbb{Z}_N : \quad 1 = s \cdot x.$

That in turn means: $\exists\, s, t \in \mathbb{Z} : \quad 1 = s \cdot x + t \cdot N.$

To decide and solve this we run the EEA

giving us r, s, t with $r = s \cdot x + t \cdot N$

and $r = \gcd(x, N)$.

We noted above that if $r \neq \pm 1$ then no solution of exists.

Thus, using (3):

$$\mathbb{Z}_{pq} \setminus \mathbb{Z}_{pq}^\times = \{ 0, p, 2p, 3p, \ldots, (q-1)p,$$
$$0, q, 2q, 3q, \ldots, (p-1)q \}.$$

Now: $\#(\ldots) = q + p - 1$

and $\#\mathbb{Z}_{pq}^\times = p \cdot q - p - q + 1 = (p-1) \cdot (q-1) = L$ ▽

Theorem Assume RSA situation, $N = pq$, $L = (p-1)(q-1)$

If $x \in \mathbb{Z}_N^\times$ then

- $x^L = 1$
- $x^{1+tL} = 1$ i.e. $x^{ed} = 1$.

And $$\frac{\#\mathbb{Z}_N^\times}{\#\mathbb{Z}_N} = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq} \simeq 1.$$

In other words: almost always $z = x$.

And in the cases where we did not prove

Missing link:

Chinese remainder theorem

Remainders modulo 15:

$\mathbb{Z}_3$ \ $\mathbb{Z}_5$	0	1 (inv.)	2	3	4 (inv.)
0	0	6	12	3	9
1 (inv.)	10	1	7	13	4
2 (inv.)	5	11	2	8	14

$x^2 - 1 = 0$

That is:

$$\mathbb{Z}_{15} \xrightarrow{\cong} \mathbb{Z}_3 \times \mathbb{Z}_5 ,$$

$$x \bmod 15 \longmapsto (x \bmod 3,\ x \bmod 5)$$

is bijective.

Counter example:

$\mathbb{Z}_4$ \ $\mathbb{Z}_6$	0	1	2	3	4	5
0	0, 12		8		4	
1		1		9		5
2	6		2		10	
3		7		3		11

$\mathbb{Z}_{24} \not\cong \mathbb{Z}_4 \times \mathbb{Z}_6$

$0 \neq 12$ but $(1,0)$

Here, 0 and 12 want the same pair in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Even more:

that map respect addition and multiplication!

Chinese Remainder Theorem

brico 10.10.14 (14)

Given m, n coprime, ie. $\gcd(m,n)=1$,
Then the map

$$\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,$$
$$x \bmod mn \longmapsto (x \bmod m,\ x \bmod n)$$

is (well-defined,) bijective and respect $+, \cdot$.

In other words:
We can find numbers x_1, x_2 by the help of EEA such that

$$\left.\begin{array}{l} x \equiv_m a \\ x \equiv_n b \end{array}\right\} \Leftrightarrow \quad x \equiv_{mn} a x_2 + b x_1.$$

The EEA (m,n) yields $\underbrace{\xi_1}_{x_1} m + \underbrace{\xi_2}_{x_2} n = 1$
since $\gcd(m,n)=1$ by assumption.

Thus

$$\begin{array}{l|l} x_1 \equiv_m 0, & x_2 \equiv_m 1-\xi_1 m \equiv_m 1 \\ x_1 \equiv_n 1-\xi_2 n \equiv_n 1 & x_2 \equiv_n 0 \end{array}$$

So

$$a x_2 + b x_1 \equiv_m a \cdot 0 + b \cdot 0 = a$$
$$a x_2 + b x_1 \equiv_n a \cdot 0 + b \cdot 1 = b$$

That is we are done.

Corollary If $\gcd(m,n)=1$:

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \qquad \square$$

Corollary Assume $\gcd(m,n)=1$. Then

$$\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$$

In particular,

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

Now, considering primes p, q, $p \neq q$:

$$\varphi(pq) = \varphi(p) \cdot \varphi(q)$$

$$\varphi(p) = p-1, \quad \varphi(q) = q-1.$$

Note that for a prime p we always have

$$\mathbb{Z}_p^{\times} = \mathbb{Z}_p \setminus \{0\}.$$

In other words: $\mathbb{Z}_p$ is a field $=: \mathbb{F}_p$.

Side remark: $\mathbb{Z}_4$ is not a field!
But a field $\mathbb{F}_4$ with 4 elements does exist. (See above!)

In particular: $\varphi(p) = p-1$.

Moreover: Let $L = (p-1)(q-1)$.
Then $x^{1+kL} = x$ in $\mathbb{Z}_{pq}$.

Proof $x^{1+kL} = x$ in $\mathbb{Z}_p$ since $x^{1+k(q-1)(p-1)} = x \cdot (x^{p-1})^{k(q-1)} = \begin{cases} 0 \cdot 0^{k(q-1)} = 0 \\ x \cdot 1^{k(q-1)} = x \end{cases}$

Bottom line:

RSA is correct in all cases!

How to recognize a prime?

Observations:

- $\mathbb{Z}_m$ is a field $\Leftrightarrow$ m prime

* if p, q are prime then $x^2 - 1 = 0$ has four(!) solutions over $\mathbb{Z}_{pq}$.

(Strong) Fermat test (Miller ; Rabin)

bnco 10.10.14 (17)

Input: a number $m \in \mathbb{Z}$

Output: a verdict, either: "m is not prime"
or "m may be prime".

1. Pick $x \in_R \mathbb{Z}_m \setminus \{0\}$ at random.
2. If $x \notin \mathbb{Z}_m^\times$ i.e. $\gcd(x,m) \neq 1$
   then "m is not prime" (and we have a factor).
3. Write $m-1 = 2^s \cdot \lambda$ with λ odd.
4. Compute $b_0 = x^\lambda$ (by square & multiply)
   $b_1 = x^{2\lambda}$
   $b_2 = x^{2^2\lambda}$
   $\vdots$
   $b_s = x^{2^s\lambda} = x^{m-1}$
   } in $\mathbb{Z}_m$.
5. If $b_s \neq 1$ then "m is not prime".
6. If $b_0 = 1$ then "m may be prime".
7. Say $b_t \neq 1$, $b_{t+1} = 1$.
   If $b_t \neq -1$ then "m is not prime"
   (and we can tell a factor).
8. "m may be prime".

Theorem If m is prime, the algo answers "m may be prime"
If m is not prime then the algo says "m may be prime" with probability at most $1/4$.

△

Security?

Brico
10.10.14
(18)

- If an attacker can compute p, q from N then RSA is broken completely.

- If an attacker can compute $\varphi(N)$ from N then he can derive p, q.

$$(x-p)\cdot(x-q) = x^2 - \underbrace{(p+q)}_{N-\varphi(N)+1}x + \underbrace{pq}_{N}$$

And so given $\varphi(N)$ we just need to solve $ed-1 = t\cdot\varphi(N)$ ...
is too costly.

Given two key pairs:

$ed-1$
$e'd'-1$

are both multiples of $\varphi(N)$ $\Rightarrow$ $\gcd(ed-1, e'd'-1)$ as well.

- Assume an attacker can decrypt given only $(N, e, y) \longmapsto x$.
  Can she also find d? Or $\varphi(N)$?
  Or p, q?

There are some approaches...

↑ Hofheinz, Kiltz & Shoup.