Lecture Notes

Foundations of informatics — a bridging course
Mathematical tools

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Fall 2012

Foundations of informatics — a bridging course
Fall 2012
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 exactly all lights are on. (Maybe there's a cord that is hit by focussed light beams from the lamps, but it'll burn only...)

(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.

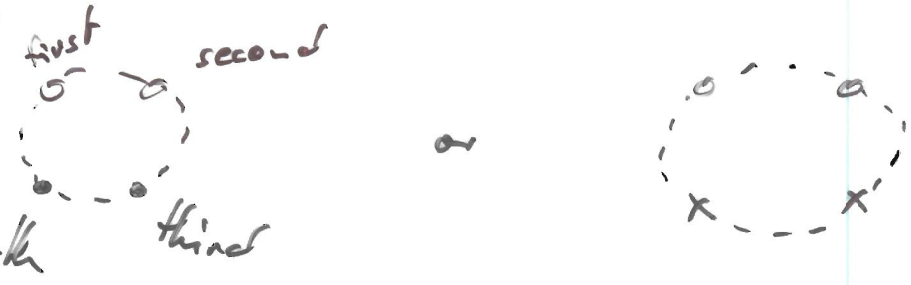
Next morning, the five divide the remaining coins equally among them without any spare coin.

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.

Ex 1.1

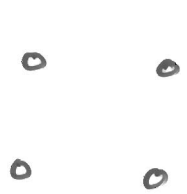
2012/10/8
(1)
bnco

(a)



- Tanya's solution:
  - switch the first:

  - switch the second:



  found by trial-and-error

- Alternative ways to find it:
  - brute force (i.e. try all possibilities). [Adel]

    Usually: brute force is no solution.

  Q: How many possibilities would we have to check here?

  - inverse trial-and-error,
  - actually meet-in-the-middle. [Anton]

- Andrii's solution

Anton's solution

2012/10/18
brico
(2)

Observations and hypotheses

- Anton: turn on/off only lamps that were off.
  - always adjacent to an a lit lamp.
  - almost always
- Ravi: we could exchange the last two moves in Anton's solution.
- Alan: you need to get into a state where only three adjacent lamps are off.
- ... multiple of three ...

Notation

Anton: use 0 and 1 for off and on, resp.

Ravi: use numbers and dots

Krishna: use − and + for off and on, resp.

✗	✓
-1	+1

- 0, 1 look particularly attractive because you can do further operations on them.
- Same for −1, +1.
- We can put numbers into a matrix or a vector.
- ~~We are~~ Boolean operations ...
- ... kind of an XOR ...

Q: How to keep doing that together?

Khalid: Claim The number of lamps must be a power of 3 plus 1, i.e. $3^k + 1$, to be able to escape in the non-trivial starting settings.

2012/10/08 brico (3)

.... ?

Adèl: Claim Given that we start at (5)

let $x \geq 5$ be # of lamps → (1)

- $x \% 3 = 2$
- ~~any two adjacent lamps should be turned on~~ → (2)
- assume that only 2 lamps are on and the rest are off. These 2 lamps should be adjacent.

⇒ Given the above hypothesis, the problem is solvable.

TRUE

↓: # starting positions with x lamps $= 2^x$.

Suparno: the above claim also holds if $x \% 3 = 1$.

Anton: also for $x \% 3 = 0$ there are solvable cases.

⇒ We should better generalise the considered starting situation

2021/10/04
brico
(4)

Andrii: Use symmetry!

↳ Only a bit more than $\frac{2^x}{2x}$ cases to consider.

☺ less than before.

☹ still too much

Uwe: Use XOR to get from one state to another.

States: A situation is coded by a vector of 0 and 1, meaning that lamp i is lit iff $v_i = 1$

Rules: Each move is given by ~~XORing~~ adding modulo 2 the vector with a certain vector t_i, which has three adjacent 1s at positions $i-1, i, i+1$.

Example:

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix} + t_1 + t_2 = \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

t_1: $\begin{bmatrix}1\\1\\0\\1\end{bmatrix}$ ← 1 $\quad$ t_2: $\begin{bmatrix}1\\1\\1\\0\end{bmatrix}$ ← 2

starting situation

state of all lamps lit!

Ex

state | switch

0 0 1 0 1 | 1 1 1 0 0 1

↳ Rules

over $\mathbb{Z}_2$

Our example:

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix} + 1\cdot\begin{bmatrix}1\\1\\0\\1\end{bmatrix} + 1\cdot\begin{bmatrix}1\\1\\1\\0\end{bmatrix} + 0\cdot\begin{bmatrix}0\\1\\1\\1\end{bmatrix} + 0\cdot\begin{bmatrix}0\\1\\1\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

start — move1 — move2 — move3 — move4 — target

STATEMENT

The order of the used moves is not important.

Note XOR is addition modulo 2.

Excursion:

$\mathbb{Z}_2 = (\{0,1\}, +)$ is a commutative group.

+	0	1
0	0	1
1	1	0

addition modulo 2.

Properly def: it's a set S with a binary operation $+ : S \times S \to S$

Associative: $\forall a,b,c \in S: (a+b)+c = a+(b+c)$

Neutral: $\exists 0 \in S\ \forall a \in S: a+0 = a \wedge 0+a = a$

Inverse: $\forall a \in S\ \exists b \in S: a+b = 0 \wedge b+a = 0$

Commutative: $\forall a,b \in S: a+b = b+a$

$\mathbb{Z}_2 = (\{0,1\}, +, \cdot)$ is a field.

·	0	1
0	0	0
1	0	1

multiplication modulo 2

Properly def: it's a set with a binary op. $\cdot : S \times S \to S$

Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Neutral: $\exists 1 \in S \ \forall a \in S: \ 1 \cdot a = a \wedge a \cdot 1 = a.$

Inverse: $\forall a \in S \setminus \{0\}: \exists b \in S: \ a \cdot b = 1 \wedge b \cdot a = 1.$

Commutative: $\forall a, b \in S: \ a \cdot b = b \cdot a$

Distributive: $\forall a, b, c \in S: \ (a+b) \cdot c = a \cdot c + b \cdot c$, $a \cdot (b+c) = a \cdot b + a \cdot c$

ØN'T: $0 \neq 1$.

Examples: $\mathbb{Z}_2$ is a field.

$\mathbb{Z}_m$ is a field if m is prime.

$(\{0, 1, \dots, m-1\}, +, \cdot)$

addition modulo m ; multiplication

Theorem

If a move occurs twice in a solution we can cancel these.

Proof

Let s be the starting situation and $i_1, \dots, i_r$ the moves that lead to escape.

Then $\text{lhs} = (\dots((s + t_{i_1}) + t_{i_2}) + \dots) + t_{i_r} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$.

Say, $i_a = i_b$.

Then, by interchanging A and C, we obtain:

$$\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \text{lhs} = s + t_{i_1} + \dots + t_{i_{a-1}} + t_{i_{a+1}} + \dots + t_{i_{b-1}} + t_{i_a} + t_{i_b} + \dots$$

$$= ((s + t_{i_1}) + \dots + t_{i_{a-1}} + t_{i_{a+1}} + \dots + t_{i_{b-1}}) + 0 + \dots$$

$((a+b)+c)+d$
$(a+(b+c))+d$
$(a+(c+b))+d$
$((a+c)+b)+d$
$(a+c)+(b+d)$
$(a+c)+(d+b)$

□

Theorem

The order of the moves does not matter

Pf: Use $A \not\parallel C$ again. □

Example

The long solution: 3, 2, 1, 3

reduces to 2, 1

or 1, 2 which is our first solution.

Now, every solution is equivalent to one operating each switch 0 or 1 times and operating all in switches in the order of their numbers.

In particular, there are only 2^x candidates for solutions.

Our example can now written as follows:

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix} + \underbrace{\begin{bmatrix}1&1&0&1\\1&1&0&0\\0&1&1&1\\1&0&1&1\end{bmatrix}}_{\text{moves}} \cdot \underbrace{\begin{bmatrix}1\\0\\0\end{bmatrix}}_{\text{solution!}} = \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

start target

Solve this equation by Gaussian elimination a the Gauß-Jordan-algorithm.

Runtime is in $O(x^3)$. FAST!

Since the matrix is sparse there are faster solutions.

Let's try to solve the second example.

$$\begin{bmatrix}1\\0\\1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1&0&0&0&1&1\\1&1&0&0&0&0\\0&1&1&0&0&0\\0&0&1&1&0&0\\0&0&0&1&1&0\\1&0&0&0&1&1\end{bmatrix} \cdot \begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\\1\\1\end{bmatrix}$$

Let's solve this using the Gauß-Jordan algorithm.
We may

- swap rows
- multiply a row with an invertible constant (non-zero when working over a field)
- add a multiple of one row to another one.

We now do it:

$$\left[\begin{array}{cccccc|c}
\boxed{1}&1&0&0&0&1&0\\
\boxed{1}&1&1&0&0&0&1\\
0&1&1&1&0&0&0\\
0&0&1&1&1&0&1\\
0&0&0&1&1&1&1\\
1&0&0&0&1&1&1
\end{array}\right]
\begin{array}{l}
\leftarrow \text{multiply by } 1^{-1}=1\\
\leftarrow \text{add modified row } -\boxed{1} \text{ times}\\
\\
\\
\leftarrow \text{add first row } -1 \text{ times}\\
\\
\leftarrow \text{add}
\end{array}$$

$$\left[\begin{array}{cccccc|c}
\boxed{1}&1&0&0&0&1&0\\
0&\boxed{0}&1&0&0&1&1\\
0&\boxed{1}&1&1&0&0&0\\
0&0&1&1&1&0&1\\
0&0&0&1&1&1&1\\
0&1&0&0&1&0&1
\end{array}\right]
\begin{array}{l}
\leftarrow \text{add}\\
\\
\\
\\
\\
\leftarrow \text{add}
\end{array}$$

swap these

multiply by $1^{-1}=1$

$$\left[\begin{array}{cccccc|c}
\boxed{1}&0&1&1&0&1&0\\
0&\boxed{1}&1&1&0&0&0\\
0&0&\boxed{1}&0&0&1&1\\
0&0&1&1&1&0&1\\
0&0&0&1&1&1&1\\
0&0&1&1&1&0&1
\end{array}\right]$$

$$\left[\begin{array}{cccccc|c}
\boxed{1}&0&0&1&0&0&1\\
0&\boxed{1}&0&1&0&1&1\\
0&0&\boxed{1}&0&0&1&1\\
0&0&0&\boxed{1}&1&1&0\\
0&0&0&1&1&1&1\\
0&0&0&1&1&1&0
\end{array}\right]$$

$$\left[\begin{array}{cccccc|c}
\boxed{1}&0&0&0&1&1&1\\
0&\boxed{1}&0&0&1&0&1\\
0&0&\boxed{1}&0&0&1&1\\
0&0&0&\boxed{1}&1&1&0\\
0&0&0&0&\boxed{0}&0&\boxed{1}\\
0&0&0&0&0&0&0
\end{array}\right]$$

This system has no solution since

$$\underbrace{0\cdot x_1 + \ldots + 0\cdot x_6}_{=0} = 1$$

can never be true.

12/10/08
brico
(3)

General answer

If $x \not\equiv_3 0$, i.e. $x \% 3 \neq 0$,
then every state has a solution.

If $x \equiv_3 0$, i.e. $x \% 3 = 0$, i.e. x divisible by 3,
then exactly half the states have a solution
and the other half has no solution.

Let's consider x divisible by 3.
Then the number of lamps lit in the starting situation must be divisible by 3 to allow two solutions.

Proof

Let $\ell_3(v) =$ (# of lit lamps described by the state vector v) modulo 3

Notice that $\ell_3\left(\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}\right) = 0$.

Now, if we perform a move, then we make the transition from a state v to a state w by an equation: $v + t_i = w$.

$$\ell_3(v) = \ell_3(w) \Leftarrow \begin{matrix} \vdots & \vdots & \vdots \\ 0 & 0 & \to 0 \end{matrix}$$

$$= \ell_3(w) + 1.$$

$$= \ell_3(w) - 1$$

Counter example: $t_2 + t_3 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$ has $\ell_3 = 2$.

Let's at least prove that in case X is divisible by 3 there are unsolvable cases:

12/10/08 bico (20)

Notice that $\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}$ vector results in changing all lights

and $\begin{bmatrix}1\\0\\1\\0\\\vdots\end{bmatrix}$ also.

Thus $\begin{bmatrix}0\\1\\0\\1\\\vdots\end{bmatrix}$ changes no light!

Actually, $\begin{bmatrix}0\\0\\\vdots\end{bmatrix}, \begin{bmatrix}0\\1\\\vdots\end{bmatrix}, \begin{bmatrix}1\\0\\\vdots\end{bmatrix}, \begin{bmatrix}1\\1\\\vdots\end{bmatrix}$ all do not change the state.

The problem is a square system:

$$A\mathbf{x} = b \quad \text{with } A \text{ square.}$$

and A has a two-dimensional kernel:

$\{\mathbf{x} \mid A\mathbf{x} = 0\}$ has $\dim = 2$,
i.e. four elements over $\mathbb{Z}_2$

Thus $\text{range } A = \{A\mathbf{x} \mid \mathbf{x}\}$

has dimension $x-2$ which is smaller
than entire space dimension x.

Both the Gauß-Jordan algorithm and the Gaussian elimination have run time $O(n^3)$ operations in the ground field for an $n \times n$ system.

Volker Strassen (1969) Gaussian elimination is not optimal.

usually, # op's (multiplications) $= 8 = 2^3$.

Now, V. Strassen was the first to find an algorithm to do this without needing commutativity in 7 multiplications:

$$\#\ \text{op's in best algo} \leq 7 = 2^{\log_2 7}.$$

Using that inductively we obtain

$$\leq 2^{2.83}$$

$$\text{Matrix Multiplication}(n) \in O(n^{2.83}).$$

Many improvements during the following 10/15 yrs:

Coppersmith & Winograd (1990)

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

Conjecture: It's actually $O(n^{2+\varepsilon})$ for any $\varepsilon > 0$.

Another example for Gauß-Jordan:

2012/10/05
bric
(2)

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

Rem Gauß-Jordan:

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

This matrix already is in (strong) row-echelon-form.

A b

Pivot elements.

The Gauß-Jordan algorithm always ends with a matrix in this row-echelon-form.

How to read off the solutions? By Expansion:

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

← new row
old first row
← new
← new
old second row
← new
← new
old third row
← new

v_4 v_3 v_5 v_6 v_7 v_8 w

These columns fulfill $Ax = 0$.

This fulfills $Ax = b$.

A test:

$$\begin{bmatrix} 0 & 1 & 3 & -2 & 0 & 2 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 5 \\ 0 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 3 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0$$

Actually, all the -1 columns (v_i) are linearly independent,

ie. if $\sum_i \alpha_i v_i = 0 \Rightarrow \forall i : \alpha_i = 0$.

Moreover, the -1 columns span* all the entire kernel of A.

$\ker A = \{x \mid Ax = 0\}$

this is a vector space!

Now, we actually want to solve $Ax = b$.

* ie. $\ker A = \{ \sum \alpha_i v_i \mid \alpha_i \in \mathbb{F}_7 \}$.

Let's test the last column

$$A \cdot \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ 3 \\ 0 \end{bmatrix}}_{=: w} = 1 \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + 2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + 3 \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 0 \end{bmatrix} = b.$$

Thus

$$\{x \mid Ax = b\} = \left\{ w + \sum_{i \in \{1,3,4,6,7,9\}} \alpha_i v_i \mid \alpha_i \in \mathbb{F}_7 \right\}$$

This is the entire story!

WARNING: Expansion only works correctly after Gauß-Jordan.

~~Rec~~

· A vector space is ...

PANIC$^+$ $\qquad +: V \times V \to V$

PAN D for scalar multiplication $\cdot : F \times V \to V$

Easiest vector spaces are F^n where $n \in \mathbb{N}$.

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

A matrix A describes a 'nice' map: $f: V \to W$,

nice = linear, i.e. $f(v+w) = f(v) + f(w)$,

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

and $\qquad f(v) = A \cdot v$

Every vector space V has a Basis,

ie. a list $(b_1, \ldots, b_m)$ such that

$(b_1, \ldots, b_m)$ span V

and

$(b_1, \ldots, b_m)$ lin. indep.,

and each such basis has the same cardinality / length: it's called its dimension.

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

then $\qquad \ker A = \{ x \in F^m \mid Ax = 0 \text{ in } F^n \}$

is a vector space (over F).

and

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

is also a vector space (over F).

2012/10/05
brico
(5)

Theorem

$$\dim \ker A + \dim \operatorname{im} A = n$$

(n = number of columns of A.)

Proof Interpret the row-echelon form of A:

$\ker A$ has the expanded -1 columns as a basis, so

$\dim \ker A$ = n - # Pivots

~~dim im~~

$\operatorname{im} A$ has those columns as a basis which transform into the Pivot columns during the Gauß-Jordan algorithm, so

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

□

Let's consider another example:

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

Excursion:

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

(4 5 6)

To have the entire multiplication:

$\cdot$	1	2	3
1	1	2	3
2	2	-3	-1
3	3	-1	2

And

a	1	2	3
a^{-1}	1	-3	-2

So let's do it:

$$\left[\begin{array}{cccc|c} -1 & 2 & 3 & 0 & 1 \\ 3 & 1 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & -2 \end{array}\right] \begin{matrix} \cdot \text{ mult by } (-1)^{-1} = -1 \\ \text{add mod. row multiplied by } +3. \\ \\ \end{matrix}$$

$$\left[\begin{array}{cccc|cc} 1 & -2 & 3 & 0 & -1 & -1 \\ 0 & 0 & 2 & 2 & -2 & -2 \\ 0 & 0 & 2 & 2 & -2 & 3 \end{array}\right] \begin{matrix} \\ \cdot \text{ subtract mod. row } -3 \text{ times} \\ \cdot \text{ mult by } 2^{-1} = -3 \\ \cdot \text{ subtract mod. row } 2 \text{ times} \end{matrix}$$

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

Now expand:

$$\left[\begin{array}{cccc|c} 1 & -2 & 0 & 3 & 3 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ & v_2 & & v_4 & w \end{array}\right] \begin{matrix} \leftarrow \text{ old first} \\ \leftarrow \text{ new} \\ \leftarrow \text{ old second} \\ \leftarrow \text{ new} \\ \\ \end{matrix}$$

So the set of solutions

$$\{ x \in \mathbb{F}_7^4 \mid Ax = b \} = \left\{ \begin{bmatrix} 3 \\ 0 \\ -1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} -2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 3 \\ 0 \\ 1 \\ -1 \end{bmatrix} \mid \alpha_2, \alpha_4 \in \mathbb{F}_7 \right\}.$$

For the second right hand side we find $0 = 1$ due to the pivot on the right and thus it is no solution.

2012 / 10 / 09
bric
(7)

Exercises

(A) Solve

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

with $b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$ and also with $b_2 = \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix}$.

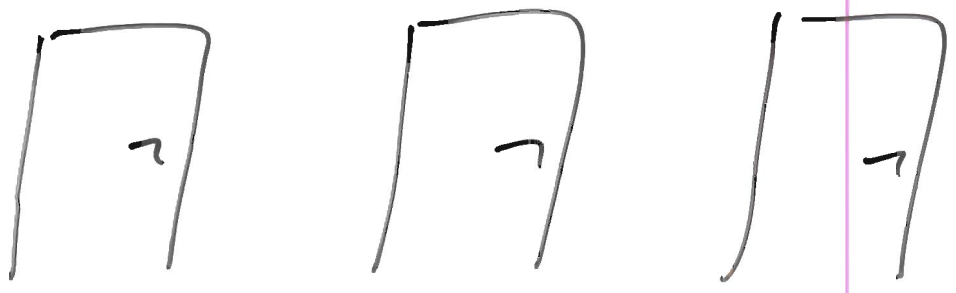
(B) Solve

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

(C) Solve Ex 1.2.

Monty Hall Problem

2012/10/09
brico
(8)



- Candidate chooses one door.
- Then Monty Hall opens one of the remaining doors and reveals a goat.

- The candidate now has the option to switch to the remaining other closed door.

What shall she do?

(A)

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

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

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

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

Thus $Ax = b_1$ is solvable and expands to

$$\left[\begin{array}{cccc|c} 1 & 2 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right] \qquad (v_2, v_4, w)$$

and the solutions are

$$\mathcal{L}\{Ax = b_1\} = \left\{ \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 1 \\ 0 \\ 2 \\ -1 \end{bmatrix} \;\middle|\; \alpha_2, \alpha_4 \in \mathbb{F}_7 \right\}.$$

(w, v_2, v_4)

Since the b_2 column is Pivot, i.e. we obtain $0x = 1$, there is no solution for $Ax = b_2$.

(B)

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

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

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

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

← ✓ There are solutions:

Expanding gives

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

so $\mathcal{L}\{x \mid Ax = b\} = \left\{ \begin{bmatrix} 2 \\ -1 \\ 1 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \;\middle|\; \alpha_4 \in \mathbb{F}_7 \right\}$

2012/10/09
brico
(10)

Ex 1.2

Translate the game into some formalism:

States Each player i has a certain number v_i of cards.
The vector $v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ is a state.

Moves Player i gives away 2 cards, 1 to the left and 1 to the right,
ie. state v is transformed into state w
by
$$v + t_i = w$$
where
$$t_i = \begin{bmatrix} \vdots \\ -2 \leftarrow i \\ \vdots \end{bmatrix}$$

Target A state where each entry is a multiple of m.

The problem translates into:

(A) Find $k \in \mathbb{Z}_m^n$ such that

$$s + T \cdot \underline{k} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad \text{over } \mathbb{Z}_m.$$

(s: starting state; (always a ring))

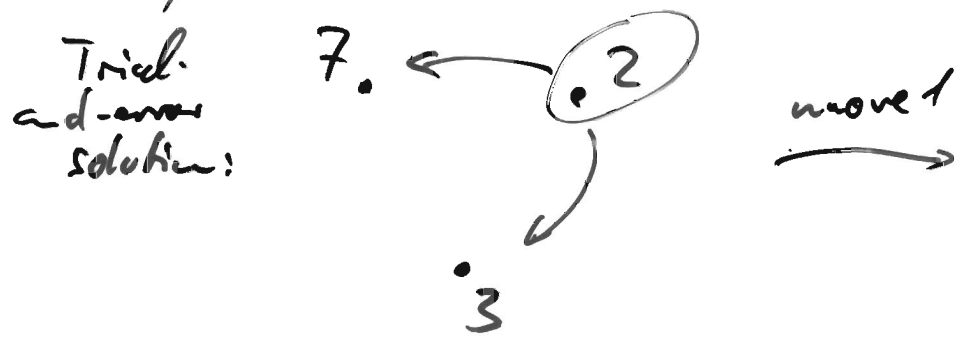
where $T = [t_1 | t_2 | \dots t_n] \in \mathbb{Z}_m^{n \times 4}$, $s \in \mathbb{Z}_m^{n}$.

(B) Find $K \in \mathbb{N}^n$ such that
$K \bmod m = k$
$s + T \cdot K \in (m\mathbb{N})^n$.

(abusing notation for s, T: $s \in \mathbb{N}^4$, $T \in \mathbb{Z}^{n \times 4}$).

1.2 (i)

Trial-and-error solution:



Problem: modules $m = 4$ is not prime

~~Linear~~ linear algebra is much more complicated!

1.2 (ii) $n = 3$, $m = 5$, $v = \begin{bmatrix} 2 \\ 3 \\ 7 \end{bmatrix}$.

Here the total number of jobs is 12 which is not a multiple of $m = 5$. Thus there can be no solution... (Intuition here. Proof in formalism needed!)

1.2 (iii) A done, see above.

Solutions for k are

$$\begin{bmatrix} -2 \\ 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ -3 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ -2 \\ 3 \\ -3 \end{bmatrix}, \begin{bmatrix} 3 \\ -1 \\ -3 \\ -2 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ -2 \\ -1 \end{bmatrix}.$$

$s = \begin{bmatrix} 2 \\ 5 \\ 11 \\ 3 \end{bmatrix}$

For k:

$$\begin{bmatrix} 5 \\ 1 \\ 6 \\ 0 \end{bmatrix} + (7N)^4, \ldots \qquad \underbrace{\begin{bmatrix} 0 \\ 3 \\ 1 \\ 2 \end{bmatrix} + (7N)^*}_{\text{most promising candidate.}}, \ldots$$

target $= \begin{bmatrix} 7 \\ 0 \\ 14 \\ 0 \end{bmatrix}$.

2012/10/10
brico
(1)

So far: linear algebra, Gauß-Jordan, modelling real situations...

Leftovers: (i) determinant and how to compute it
(ii) inverse matrix

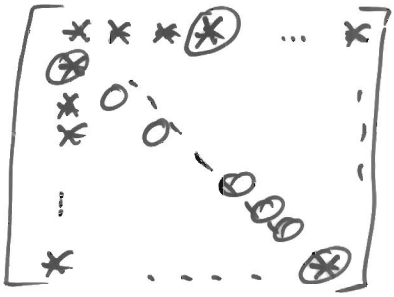
ad (i)

Given $A \in F^{n \times n}$, a square matrix over a field F, we would like to have 'simple' expression that tells us whether or not A has an inverse...

We define:

$$\det A = \sum_{\pi \in S_n} (-1)^{\operatorname{sgn}(\pi)} \prod_{0 \le i \le n-1} A_{i,\pi(i)} \qquad (*)$$

$$A = [\, A_{ij} \,]_{0 \le i,j \le n-1}$$



permutation of n elements,

i.e. $\pi : \{0, \dots, n-1\} \longrightarrow \{0, \dots, n-1\}$

bijective (i.e. injective & surjective)

The parity / signum $\operatorname{sgn}(\pi)$ tells whether the number of swaps needed for describing π (in one or all cases, resp.) is even or odd:

$$\operatorname{sgn}(\pi) = \begin{cases} 0, & \text{if \#swaps even,} \\ 1, & \text{if \#swaps odd.} \end{cases}$$

Properties

- $\det A$ invertible $\Leftrightarrow$ A invertible
  (non-zero)
- $\det \mathbb{1} = 1$
  ↑ identity matrix
  unit matrix
  $\mathbb{1} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$
- $\det(AB) = \det A \cdot \det B$.
- if B is the matrix A with the two rows k, l swapped
  then $\det B = -\det A$.
- if B is the matrix A with row k scaled by the constant c
  then $\det B = c \cdot \det A$.
- if B is the matrix A with row k replaced with the row k plus a multiple of row l
  then $\det B = \det A$.

2012/10/10
bnico
(3)

How to compute the determinant?

(a) using the definition:

- for each product $\prod_{0 \le i < n} A_{i,\pi(i)}$
  we need $n-1$ multiplications in $\mathbb{F}$.
- the number of summand, i.e. the number of ~~previous~~ executions of the previous step, is the number of permutations: $\# \mathcal{S}_n$.

$$\# \mathcal{S}_n = n!$$

$$\left[\# \mathcal{S}_0 = 1, \quad \# \mathcal{S}_n = n \cdot \# \mathcal{S}_{n-1}, \dots \right]$$

Thus we need

$$(n-1) \cdot n! \in \Theta(n^n) = \Theta(2^{n \log n})$$

multiplications in $\mathbb{F}$ to evaluate (*).

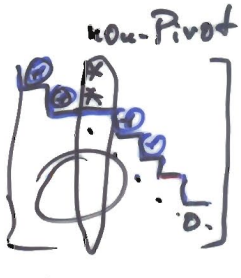
That is very, very slow.

(b) use the properties and the Gauß-Jordan algorithm.

Notice: the determinant of a square matrix in row-echelon-form is

(i) 1 if the row-echelon-form is $\mathbb{1}$.

(ii) 0 otherwise.



So follow the Gauß-Jordan algorithm and for each swap note/accumulate a -1 and for each scaling by a constant c note/accumulate a c^{-1}

If we arrive at $\mathbb{1}$, i.e. (i),
then the product of the naked
numbers is $\det A$,
Otherwise $\det A = 0$.

As a side result we obtain:

$Ax = b$ is always solvable (for any b)

$\Leftrightarrow$

A is invertible

$\Leftrightarrow$ $\det A$ is non-zero (invertible).

Price / runtime for this second solution?

Gauß-Jordan algorithm: $O(n^3)$

additional bookkeeping: $O(n)$

$O(n^3)$.

Examples

$$\det \begin{bmatrix} -2 & 1 & 0 & 1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{bmatrix} = 0 \qquad \text{(see above)}$$

$$\det \begin{bmatrix} 3 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & -2 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix} = 3 \cdot (-1) \cdot (-2) \cdot 1 \cdot 1 \text{ over } \mathbb{F}_7.$$

$$= -1.$$

GJ:

$$\left(\begin{array}{cccc|cccc} 3 & 1 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & -2 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & -2 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & -2 & 1 & -3 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 2 & 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & -2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

2012/10/10
trio (5)

Ex (5)

Compute the determinant of the matrix

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

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

$$\begin{array}{ccccc} 1 & 1 & 3 & 2 & 0 \\ 0 & -2 & 2 & 3 & 0 \\ 0 & -1 & -2 & 0 & 1 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 1 & 0 & 3 & 1 \end{array} \qquad \cdot \frac{1}{-2} = 3$$

$$\begin{array}{ccccc} 1 & 0 & -3 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 \\ 0 & 0 & -3 & 2 & 1 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 4 & -2 & 1 \end{array} \qquad \cdot \frac{1}{-3} = 2 \qquad -2 \cdot -3 = -1$$

$$\begin{array}{ccccc} 1 & 0 & 0 & -2 & -1 \\ 0 & 1 & 0 & -1 & 2 \\ 0 & 0 & 1 & -3 & 2 \\ 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 2 & 2 \end{array} \qquad \cdot \frac{1}{-2} = 3 \qquad -1 \cdot -2 = 2$$

$$\begin{array}{ccccc} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 3 \end{array} \qquad \cdot \frac{1}{3} = -2 \qquad 2 \cdot 3 = -1$$

$$\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}$$

$$-1 \cdot \boxed{-1} = -1$$

~~$\det A = -1$~~

$\det A = 2$

2012/10/10
hw8
6

```
[d,B]:=gaussjordan(A,MZ7(5,0)):
Starting.
```

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

```
Pivoting column 1.
```

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

```
Scaling row 2 by 3.
```

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

```
Pivoting column 2.
```

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

```
Scaling row 3 by 2.
```

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

```
Pivoting column 3.
```

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

```
Scaling row 4 by 3.
```

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

```
Pivoting column 4.
```

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

```
Pivoting column 5.
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

```
Completed. det(A)= 2.
```

Ad (iii) How to compute the inverse matrix if it exists ...

Given $A \in F^{n\times n}$ a square matrix over some field F
then $B \in F^{n\times n}$ is its inverse iff

$$A \cdot B = \mathbb{1}$$

(and $B \cdot A = \mathbb{1}$).

We write $A^{-1} := B$.

Fact A^{-1} exists iff $\det A \neq 0$ (invertible)

If A^{-1} exists then $Ax = b$ is solvable for any b:
The $Ax = b$ is equiv. to $A^{-1}Ax = A^{-1}b$
$x = \mathbb{1}x$

Thus $\det A \neq 0$.

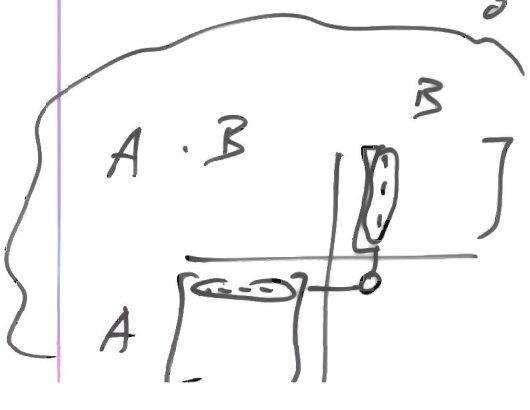
On the other hand assume $\det A \neq 0$.
Then $Ax = b$ is solvable for all b.
In particular, we may pick b as a unit vector u_i.
Then we find x_i such that $Ax_i = u_i$.

Now: $A \cdot [x_1 | \dots | x_n] = [u_1 | \dots | u_n] = \mathbb{1}$.

Thus $A^{-1} = [x_1 | \dots | x_n]$.

This is equiv. to
$A^T \cdot B^T = \mathbb{1}^T = \mathbb{1}$.
This is solvable iff $\det A^T \neq 0$
$\det A$.

If you have $AB = \mathbb{1}$ and $CA = \mathbb{1}$
then $C = C \cdot \mathbb{1} = C(AB) = (CA)B = \mathbb{1} \cdot B = B$.



2012/10/10
Nico
(8)

Now, the above proof also shows how to compute the inverse of A:

Write down

$$A \mid \mathbb{1}$$

and run Gauß-Jordan.

You obtain

$$\mathbb{1} \mid B$$

provided A is invertible. This B is the inverse A^{-1}.

2012/10/10
brico
(9)

```
[d,B]:=gaussjordan(A,MZ7(5,5,(i,j)->if i=j then 1 else 0 end_if)):
Starting.
```

$$\left(\begin{array}{cccc|ccccc} 1 & 1 & 3 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 3 & -2 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

```
Pivoting column 1.
```

$$\left(\begin{array}{ccccccccccc} 1 & 1 & 3 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 2 & 3 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & -1 & -2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right)$$

```
Scaling row 2 by 3.
```

$$\left(\begin{array}{ccccccccccc} 1 & 1 & 3 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & -1 & -2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right)$$

```
Pivoting column 2.
```

$$\left(\begin{array}{ccccccccccc} 1 & 0 & -3 & 0 & 0 & 0 & -3 & 0 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & -3 & 2 & 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & -2 & -3 & 0 & 0 & 1 \end{array}\right)$$

```
Scaling row 3 by 2.
```

$$\left(\begin{array}{ccccccccccc} 1 & 0 & -3 & 0 & 0 & 0 & -3 & 0 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 2 & 2 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & -2 & -3 & 0 & 0 & 1 \end{array}\right)$$

```
Pivoting column 3.
```

$$\left(\begin{array}{ccccccccccc} 1 & 0 & 0 & -2 & -1 & -1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 2 & 3 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & -3 & 2 & 2 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & -1 & 3 & -2 & -2 & 0 & 1 \end{array}\right)$$

```
Scaling row 4 by 3.
```

$$\left(\begin{array}{ccccccccccc} 1 & 0 & 0 & -2 & -1 & -1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 2 & 3 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & -3 & 2 & 2 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & -3 & -1 & 3 & -2 & -2 & 0 & 1 \end{array}\right)$$

```
Pivoting column 4.
```

$$\left(\begin{array}{ccccccccccc} 1 & 0 & 0 & 0 & -2 & -1 & 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -2 & 3 & 2 & 2 & 3 & 0 \\ 0 & 0 & 1 & 0 & -3 & 2 & -1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & -2 & -2 & 2 & 1 \end{array}\right)$$

```
Pivoting column 5.
```

$$\left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 0 & -2 & -3 & 2 & 3 & 2 \\ 0 & 1 & 0 & 0 & 0 & 2 & -2 & -2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & -3 & 0 & 3 & 1 & 3 \\ 0 & 0 & 0 & 1 & 0 & -2 & -1 & -1 & -3 & -3 \\ 0 & 0 & 0 & 0 & 1 & 3 & -2 & -2 & 2 & 1 \end{array}\right)$$

```
Completed. det(A)= 2.
```

$\rightsquigarrow A^{-1}$

How to cross check a solution after Gauß-Jordan?

Solving $Ax = b$

plug in the x you found!

Finding A^{-1}:

. check $A^{-1} \cdot A = \mathbb{1}$

(or $A \cdot A^{-1} = \mathbb{1}$).

Foundations of informatics — a bridging course
Fall 2012
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:

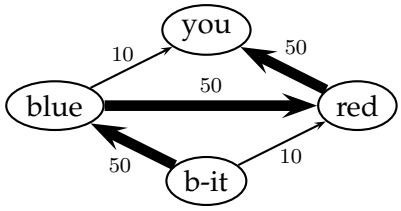


Figure 2.1: Network

(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.

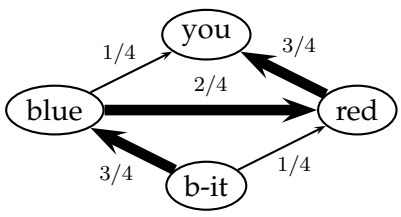


Figure 2.2: Relative flows

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 2012
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 probabilities

brico
2012/10/10
(cc)

1. Events

- A universe Ω is a set of possible outcomes of an experiment.
- An event A is just a subset of Ω, $A \subseteq \Omega$.

Rules

$$\text{prob}(\emptyset) = 0.$$

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

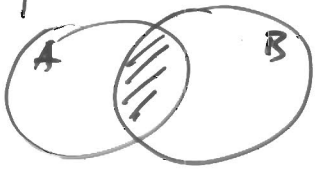
$$\text{prob}(\Omega) = 1.$$

(where $A \dot\cup B$ means $A \cup B$ and that $A \cap B = \emptyset$.)

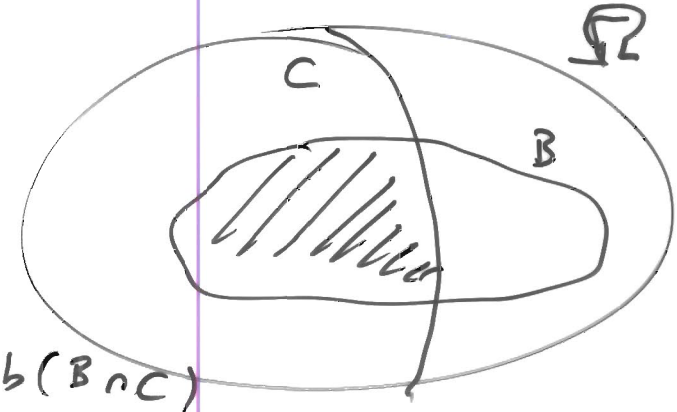
Consequence: $\text{prob}(\Omega \setminus A) = 1 - \text{prob}(A)$

$\ulcorner$ $A \dot\cup (\Omega \setminus A) = \Omega$ and thus $\text{prob}\, A + \text{prob}(\Omega \setminus A) = \text{prob}\, \Omega = 1$. $\lrcorner$

Also: $\text{prob}(A \cup B) = \text{prob}\, A + \text{prob}\, B - \text{prob}(A \cap B)$.



$\ulcorner$ ... $\lrcorner$



Conditional probabilities

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

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

Def A and B are independent

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

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

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

$C = \{2,4,6\}$,

$B = \{4,5,6\}$.

$\text{prob}\, B = \frac{1}{2}$

$\text{prob}(B \mid C) = \frac{2}{3}$))

$\frac{\text{prob}(B \cap C)}{\text{prob}\, C} = \frac{4/6}{1/2}$

(2012/10/10 bis 0 (11)

2. Random variables

Def A r.v. X is a function on the universe Ω. $X : \Omega \to S$

And we always assume that we know its distribution

$x \mapsto \text{prob}(X = x) := \text{prob}(\{\omega \in \Omega \mid X(\omega) = x\})$

$S \longrightarrow [0,1]$

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

Def Two r.v. X and Y are <u>independent</u>

$\left\{ \forall_{\substack{x \in \text{range } X \\ y \in \text{range } Y}} : \text{prob}(X = x \wedge Y = y) = \text{prob}(X = x) \cdot \text{prob}(Y = y) \right.$

Monty Hall problem:

It is good to switch!

She doubles her chances.

Random exit

(2012/10/10 brico (12))

Consider a program:

```
REPEAT
    certain stuff
UNTIL   condition C holds
```

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

For a nice solution we introduce r.v.

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

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

We want to analyse the r.v.

N = # rounds till exit.

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

So we can calculate

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

Def The expected value of a 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:

$$E(N) = \sum_{j \geq 1} j \cdot \text{prob}(N = j)$$

$$= \left(\sum_{j \geq 1} j \cdot (1-p)^{j-1} \right) \cdot p$$

$$= \frac{1}{(1-(1-p))^2} \cdot p$$

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

We know
$\sum_{j \geq 0} x^j = \frac{1}{1-x}$
for $|x| < 1$.
Its derivate is termwise
$\sum_{j \geq 0} j x^{j-1} = \frac{1}{(1-x)^2}$.
Since we have absolute convergence this all fine.

WARNING: We should actually only consider finitely many r.v.s!

Here: pick a limit b and only consider $X_1, \ldots X_b$ and a special case: none exits $\geq b$ ...

Ex 3.2

2012/10/10
Enrico
(44)

Introduce r.v.s

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

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

We know

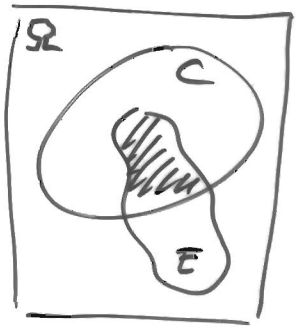
$$prob(N=1) = 0.6 = \frac{3}{5},$$

$$prob(H=1 \mid N=1) = 0.75 = \frac{3}{4},$$

$$prob(H=1 \mid N=0) = 0.25 = \frac{1}{4}.$$

We want

$$prob(N=1 \mid H=1) = ?$$



Now:

$$prob(N=1 \mid H=1) = \frac{prob(N=1 \wedge H=1)}{prob(H=1)}$$

From our knowledge we get

$$prob(N=0) = 1 - prob(N=1) = 0.4 = \frac{2}{5}$$

$$prob(H=1 \wedge N=1) = \underbrace{prob(N=1)}_{0.6} \cdot \underbrace{prob(H=1 \mid N=1)}_{0.75}$$

$$= \frac{3}{5} \cdot \frac{3}{4} = \frac{9}{20}.$$

$$prob(H=1 \wedge N=0) = prob(N=0) \cdot prob(H=1 \mid N=0)$$

$$= \frac{2}{5} \cdot \frac{1}{4} = \frac{1}{10}.$$

$$prob(H=1) = prob((H=1 \wedge N=0) \vee (H=1 \wedge N=1))$$

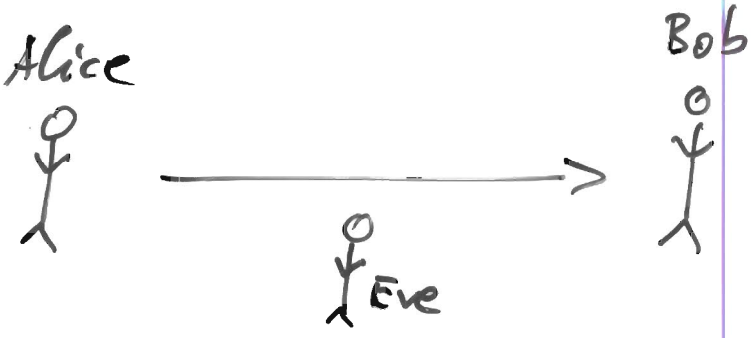
$$= prob(H=1 \wedge N=0) + prob(H=1 \wedge N=1)$$

$$= \frac{1}{10} + \frac{9}{20} = \frac{11}{20}.$$

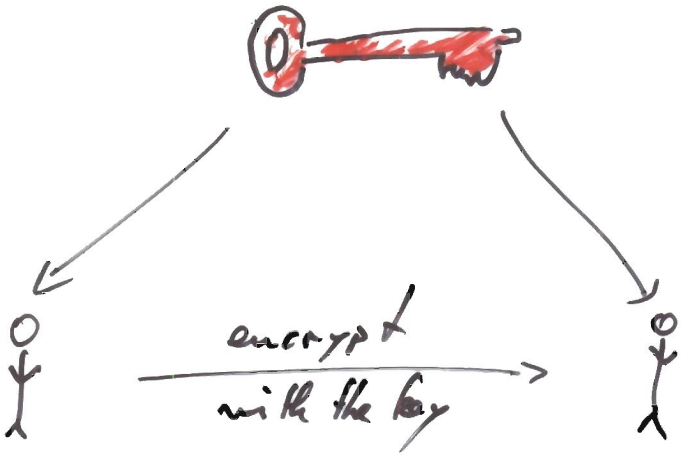
So

$$prob(N=1 \mid H=1) = \frac{9/20}{11/20} = \frac{9}{11}.$$

:)



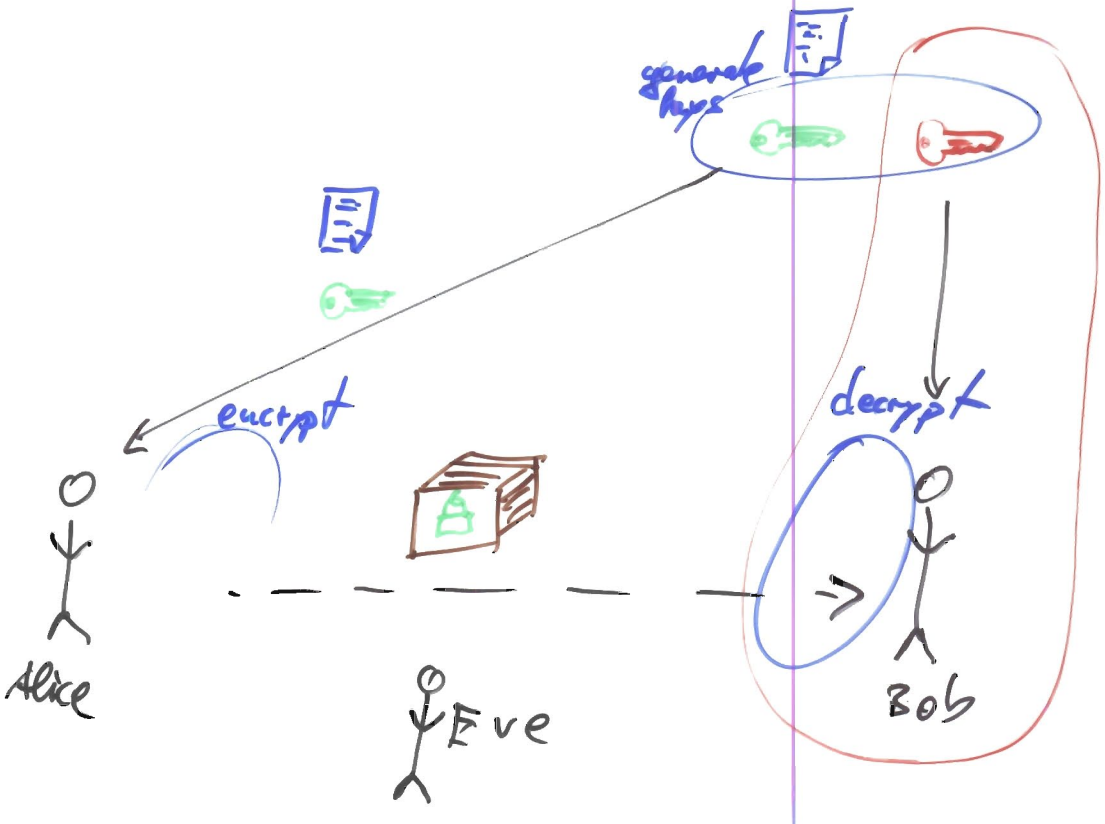
Classically



New solution [1970-72 British Secret Service]

1976 Diffie & Hellman

1978 Rivest, Shamir & Adleman : RSA.



RSA

generate_keys

Input: security parameter $k \in \mathbb{N}$.

Output: key pair

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

encrypt

Input: public key (N, e),
message $x \in \{0, \dots N-1\} = \mathbb{Z}_N$.

Output: ciphertext $y \in \mathbb{Z}_N$.

1. Return $y = x^e$ in $\mathbb{Z}_N$. $O(k^3)$

decrypt

Input: private key (N, d)
ciphertext $y \in \mathbb{Z}_N$.

Output: message $z \in \mathbb{Z}_N$.

1. Return $z = y^d$ in $\mathbb{Z}_N$ $O(k^3)$

2012/10/10
brico

Todo (0) Understand of the program.

(1) Correctness?

Is $z = x$?

(2) Efficiency?

Is everything reasonably fast?

(3) Security?

Exercise!

Integers modulo N

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

addition, multiplication modulo N.

$a +_N b := (a +_{\mathbb{Z}} b) \% N$.

$\cdot_N \quad \cdot_{\mathbb{Z}}$

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

Runtime $(+) \in \mathcal{O}(k)$

Runtime $(\cdot) \in \mathcal{O}(k^2)$

where $k = \text{length}(N) = \lfloor \log_2 N \rfloor + 1$

$\in \Theta(\log N)$

Strassen & Schönhage (1971):

Multiplication of k-bit integers can be done in $O(k \log k \log\log k)$ operations.

the construction of $\mathbb{Z}_N$ is based

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 $x \text{ rem } y := r \in \mathbb{Z}$,

$x \text{ quo } y := q$.

We also define $x \bmod y := [\mathbb{Z}_N] r \in \mathbb{Z}_N$.

Theorem Given an integer $N \geq 2$

the $\mathbb{Z}_N$ is a commutative ring (with 1),

ie. it fulfills PANIC$^+$, PANIC, DON'T

Proof (partly)

P+ : we have to check that for $a, b \in \mathbb{Z}_N$
we have $a + b \in \mathbb{Z}_N$.
— this is true by construction!
(refer to previous theorem)

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

$$\ulcorner (a \cdot_N b) \cdot_N c = [\underbrace{(a \cdot b \text{ rem } N)}_{\in \mathbb{Z}} \cdot c] \bmod N$$

$$= a \cdot b - h \cdot N \quad \text{for some } h \in \mathbb{Z}.$$

$$= [(a b - h N) \cdot c] \bmod N$$

$$= [(a \cdot b) \cdot c - hc \cdot N] \bmod N$$

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

$\cdot_{\mathbb{Z}}$ associative

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

$$\vdots$$

$$= a \cdot_N (b \cdot_N c)$$

. ⌋

ON'T: $0 \neq 1$ in $\mathbb{Z}_N$!

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

since otherwise

$$(1-0) = h \cdot N + 0$$

$$1 = h_1 \cdot N + r_1 \quad \leftarrow \text{assumption}$$
$$0 = h_0 \cdot N + r_0$$

$$1 - 0 = (h_1 - h_0) \cdot N$$

thesis $N \mid 1 \quad 1$

but $N \geq 2$ ↯.

.... □

So from now on we think of $\mathbb{Z}_N$ as a class and don't look inside any more: it's a black box.

How to compute x^e in $\mathbb{Z}_N$?
where $x \in \mathbb{Z}_N$, $e \in \mathbb{N}_{<2^k}$

The definition says:

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

Runtime: $O(e \cdot k^2)$
but: $e \in O(2^k)$
$O(k^2 \cdot 2^k)$

2012/10/11
brico
(4)

Let's assume for a moment that e can be easily factored, say $e = 2^s$.
Can we compute

$$x^e = x^{2^s}$$

better? Yes!

$$x^{2^s} = (\dots((x^2)^2)\dots)^2 \quad \text{(s times)}$$

∘∘∘

Then $x^{a+b} = x^a \cdot x^b$
$x^{a \cdot b} = (x^a)^b$
also here!

Now, take again a general e.
Write

$$e = \sum_{0 \le i < k} e_i \cdot 2^i \quad \text{(binary representation)}, \quad e_i \in \{0, 1\}.$$

Now

$$x^e = \prod_{0 \le i < k} (x^{2^i})^{e_i} = \prod_{\substack{e_i = 1 \\ 0 \le i < k}} x^{2^i}$$

at most k factors.

So we may first compute

$$x, x^2, x^{2^2}, x^{2^3}, \dots, x^{2^{k-1}}$$

and then multiply the ones together where $e_i = 1$.
This takes at most 2k multiplications in $\mathbb{Z}_N$!

$$\mathcal{O}(k^3).$$

SQUARE & MULTIPLY

Same run time but constant memory.

Slightly better; assuming $e_{k-1} = 1$:

$$x, x^2, x^{2+e_{k-2}}, x^{2^2+e_{k-2}\cdot 2}, x^{2^2+e_{k-2}\cdot 2+e_{k-3}}, \dots, x^e$$

Say $e = (101011)_2$

$$x \overset{2}{\to} x^{10} \overset{2}{\to} x^{100} \overset{\cdot x}{\to} x^{101} \overset{2}{\to} x^{1010} \overset{2}{\to} x^{10100} \overset{\cdot x}{\to} x^{10101} \overset{2}{\to} x^{101010} \overset{\cdot x}{\to} x^{101011}$$

Next question: How to perform step 5 of ~~key~~ generate_keys?
How to find e, d such that

$$e \cdot d = 1 - h \cdot L$$

with $h \in \mathbb{Z}$, $e, d \in \mathbb{Z}\mathbb{N}_{<L}$.
We try the following:

1. Repeat
2. pick $e \in \mathbb{N}_{<L}$ at random.
3. try to find $d \in \mathbb{N}_{<L}$, $h \in \mathbb{Z}$ such that
$$d \cdot e + h \cdot L = 1$$
4. Until successful

So we are left with step 3:
Notice that 1 is a very small integer.
Let's try to start easier:
Start to find numbers s, t such that

$$s \cdot e + t \cdot L$$

is small and improve on this.
Obviously, taking $s, t \in \{0, 1\}$ but not both 0 gives first finite answers:

s	t	$se+tL$
0	1	L
1	0	e

To improve we could add or subtract these repeatedly

Let's do an example:

$L = 60$ [$= (7-1)(11-1)$].

$e = 17$

r	q	s	t	comment
60		0	1	$0 \cdot e + 1 \cdot L = 60$
17	3	1	0	$1 \cdot e + 0 \cdot L = 17$
9	1	−3	−1	$-3 \cdot e + 1 \cdot L = 9$
8	1	4	−1	$4 \cdot e - 1 \cdot L = 8$
1	8	−7	2	$-7 \cdot e + 2L = 1$
0		60	−17	$60 \cdot e - 17 \cdot L = 0$

Always use the extra step as a cross check!
It's easy to verify.

This is called the

Extended Euclidean Algorithm
(EEA)

2012/10/11
brief (7)

EEA

Input: two values a, b

Output: r, s, t

1. $r_0 = a, \quad s_0 = 1, \quad t_0 = 0.$
2. $r_1 = b, \quad s_1 = 0, \quad t_1 = 1.$ $\quad i = 1.$
3. While $r_i \neq 0$ do
4. $\quad q_i := r_{i-1}$ quo r_i, (Division with remainder)
5. $\quad r_{i+1} := r_{i-1} - q_i r_i$
6. $\quad s_{i+1} := s_{i-1} - q_i s_i$
7. $\quad t_{i+1} := t_{i-1} - q_i t_i$
8. $\quad$ increment i
9. $\ell := i - 1.$
10. Return (r_ℓ, s_ℓ, t_ℓ)

Exercises

Run the EEA for starting numbers

(i) 25, 87

(ii) 22, 8

(iii) 91, 37

Further examples

r	q	s	t
60		0	1
16	3	1	0
12	1	-3	1
4	3	4	-1
0		-15	4
		$-\frac{60}{4}$	$\frac{16}{4}$

X check ok!

(i)

r	q	s	t
25		1	0
87	3	0	1
25	3	1	-3
12	2	-2	7
1	12	25	-87
0			

→ soln.
check

(ii)

22		0	1
8	2	1	0
6	1	-2	1
2	3	+3	-1
0		-11	4
		$-\frac{22}{24}$	$\frac{8}{2}$

(iii)

91		0	1
37	2	1	0
17	2	-2	1
3	5	5	-2
2	1	-27	11
1	2	32	-13
0		-91	37

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 remainders.

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

Proof: (Ex).

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

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

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

i.e.

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

$$\ell \le 2 \log_2 (\max\{|a|, |b|\}) + 1$$

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

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

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

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

(i) $d \mid a \wedge d \mid b$ (it is a common divisor)

(ii) if $c \mid a \wedge c \mid b$ then $c \mid d$.

(in particular, $|c| \le |d|$).

Proof (Fact(i)):

$$r_{i+1} = q_i r_i + r_{i+1}$$

$$r_{i-1} - q_i r_i = r_{i+1}$$

if $c \mid r_{i-1}$ and $c \mid r_i$ then c divides r_{i+1}.

if $c \mid r_i$ and $c \mid r_{i+1}$ then c divides r_{i-1}.

Thus $c \mid r_{i-1} \wedge c \mid r_i \iff c \mid r_i \wedge c \mid r_{i+1}$. □

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

$$s \cdot a + t b = 1$$

has no solution

Pf $g := \gcd(a,b) = r_e \neq \pm 1$. Now: $g \mid a \wedge g \mid b$.

Thus for any s, t also $g \mid sa + tb$.

But $g \neq 1$. ☹ □

In our very first example
the EEA produced
on input $L = 60, \quad e = 17$
the output $r = 1, \; s = -7, \; t = 2$;
ie. $1 = -7 \cdot \underbrace{17}_{e} + 2 \cdot \underbrace{60}_{L}$

$0 = 60 \cdot 17 - 17 \cdot 60$
$1 = -7 \cdot 17 + 2 \cdot 60$
$0 =$

So we find $d = -7$!.

Better take $d = 60 - 7 = 53$. $\quad 1 = 53 \cdot 17 + (2 - 17) \cdot 60$
$53 \cdot 17 + (-15) \cdot 60$

Thinking in $\mathbb{Z}_L$ also allows this.

This would into a key generation example:

1. $p = 7$ selected
2. $q = 11$ selected
3. $N = 77$
4. $L = 60$
5. $e = 17$ is selected
   and $d = 53$ computed
6. Return: $(77, 17)$ as public key,
   $(77, 53)$ as private key

Next, we should consider prime generation but we skip that for the time being.

Fact We can generate a $\frac{k}{2}$-bit prime in time $O(k^4)$

What about CORRECTNESS?

Given N, e, d from the generate-keys and any $x \in \mathbb{Z}_N$ compute

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

Is $z = x$?

Fact (to be proven)
We always have $x^{1+L} = x$
for any $x \in \mathbb{Z}_N$, $L = (p-1)\cdot(q-1)$, $N = p \cdot q$.

Corollary Also $x^{1+hL} = x$

Pf $h = 2$: $x^{1+2L} = \underbrace{x^{1+L}}_{=x} \cdot x^L = x^{1+L} = x$.

By induction the corollary follows. □

Now: $e \cdot d = 1 + hL$ for $h \in \mathbb{Z}$.

Then

$$z = x^{e\cdot d} = x^{1+hL} \overset{\text{Corollary}}{=} x .$$

!

But the above Fact is a surprise.

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

Tiny examples

$N = 15 = 3 \cdot 5$ $\quad \mathbb{Z}_N$

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

Strange: $3 \cdot 5 = 0$

multiples of 3: $0, \pm 3, \pm 6$

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

Observe $1 = 2 \cdot 4 = 8$ here. ☺

In particular: $\mathbb{Z}_{15}$ is not a field!

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

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

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

Yes: $(y^{-1}x^{-1}) \cdot (x \cdot y) = 1$. (using A2N)

A: ✓

N: 1 is invertible!

I: Yes, because the inverse of an invertible x is itself invertible.

C: ✓.

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

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: $\#\mathbb{Z}_N^\times = 8$.

another try:

$$7^8 = 4^4 = 1^2 = 1.$$

what about

$$3^8 = (-6)^4 = 6^2 = 6 \xrightarrow{\cdot 3} 3^9 = 3.$$

$3 \notin \mathbb{Z}_{15}^\times$.

Theorem (Lagrange)

Given a group G with finitely many elements. Then for any element $x \in G$ we have

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

(assuming $(G,\cdot)$ and 1 is its neutral element).

Pf in case G is commutative.

list G: $x_1, x_2, \dots, x_k$, $k = \#G$.

multiply each by x: $xx_1, xx_2, \dots, xx_k$

1. Again k elements
2. All different: $xx_i = xx_j$, then $x_i = x^{-1}xx_i = x^{-1}xx_j = x_j$. So $i=j$.
3. None missing: Take some element of G: x_i. Is it on the second list?
   Find j such that $xx_j = x_i$, but $\neq$ $x_j = x^{-1}x_i$.
   But $x^{-1}x_i$ is in G so there is such a j.

Now compare the products: (because G is commutative)

$$x_1 \cdot x_2 \cdot \ldots \cdot x_k \overset{\sigma}{=} x x_1 \cdot x x_2 \cdot \ldots \cdot x x_k$$

so:

$$\begin{array}{ccccc} 1 \cdot 1 \cdot \ldots \cdot 1 & = & x \cdot x \cdot \ldots \cdot x \\ \| & & \| \\ 1 & & x^{\#G} \end{array}$$

□

This already gives a large part of the fact from above:

now for $x \in \mathbb{Z}_N^\times$, $L = \#\mathbb{Z}_N^\times$

we have $x^{1+L} = x \cdot x^L \overset{\text{Lagrange}}{=} x \cdot 1 = x$.

and $\#(\mathbb{Z}_N \setminus \mathbb{Z}_N^\times) = p + q - 1$ ← 500 bit #

$\#\mathbb{Z}_N = p \cdot q$ ← 1000 bit #.

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 fct.)

Pf: Lagrange for G. □

Little Theorem (Fermat)

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

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

- $(x^{p-1} \equiv_p 1)$

Pf: $\varphi(p) = p - 1$. □

(2012/10/11 bis 16)

For RSA we need to determine

$$\varphi(p \cdot q) = \# \mathbb{Z}_{pq}^{\times}$$

Which elements of

$$\mathbb{Z}_{pq}$$

are not invertible?

Actually, for any $N \geq 2$:

$$\mathbb{Z}_N^{\times} = \{ x \in \mathbb{Z}_N \mid x \text{ invertible} \}$$

$$= \{ x \in \mathbb{Z}_N \mid \text{EEA}(N,x) \text{ finds an inverse} \}$$

$$= \{ x \in \mathbb{Z}_N \mid \gcd(N,x) = 1 \}.$$

Now:

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

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

i.e. $\# \mathbb{Z}_{pq}^{\times} = pq - q - p + 1 = (p-1)\cdot(q-1) = \ell$

Missing

Chinese remainder theorem

Remainders mod 15: -2 = "3", -1 = "4"

$\mathbb{Z}_3 \times \mathbb{Z}_5$	0	1	2	3	4
0	0	6	-3	3	-6
1	-5	1	7	-2	4
$-1=2$	5	-4	2	-7	-1

Be careful:

mod 4 \ mod 6	0	1	2	3 = -3	4 = -2	5 = -1
0	0, 12		8		4	
1		1		9		5
$-2=2$	6		2		10	
$-1=3$		7		3		11

$4 \cdot 6 = 24$

Theorem

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 bijective and nice wrt. to $+, \cdot$.

In other words:

We can find numbers x_1, x_2 by the help of the EEA such that

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

Actually, $x_1 = \xi m = 1 + \eta n$, $x_2 = 1 - \xi m = -\eta n$

where $\xi m - \eta n = 1$ can be solved by the EEA.

2012/10/11
brico
(18)

To find x_1, x_2 we just have to consider the cases $(a,b) = (0,1)$ and $(a,b) = (1,0)$

So: $x_1 \equiv_m 0$ and $x_1 \equiv_n 1$.

ie. $x_1 = \xi m$, $x_1 = 1 + \eta \cdot n$.

for some $\xi, \eta \in \mathbb{Z}$.

Now: $\xi \cdot m - \eta \cdot n = 1$

The EEA (m,n) will return $1, \xi, -\eta$.

Now $x_1 = \xi \cdot m = 1 + \eta n$.

Also $x_2 = 1 - \xi m = -\eta n$.

$$\left[\begin{array}{l} x_2 \equiv_m 1 - \xi m \equiv 1, \\ x_2 \equiv_n -\eta n \equiv 0 \end{array} \right]$$

Now: $\underbrace{\begin{array}{l} x_1 \equiv_m 0 \\ x_1 \equiv_n 1 \end{array}}_{\cdot b}$ $\underbrace{\begin{array}{l} x_2 \equiv_m 1 \\ x_2 \equiv_n 0 \end{array}}_{\cdot a}$

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

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

As a consequence:

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

Use this for $m=p$, $n=q$:

$$\mathbb{Z}_{pq}^{\times} \cong \mathbb{Z}_p^{\times} \times \mathbb{Z}_q^{\times}$$

so

$$\#\mathbb{Z}_{pq}^{\times} = \underbrace{\#\mathbb{Z}_p^{\times}} \cdot \underbrace{\#\mathbb{Z}_q^{\times}}$$
$$= (p-1) \cdot (q-1)$$

And

$$x^{1+L} \cong \left((x \bmod p)^{1+L}, (x \bmod q)^{1+L} \right)$$

Now:

$$(x \bmod p)^{1+2(p-1)} = \begin{cases} (x \bmod p)^{\ast} \cdot 1 & \text{if } x \bmod p \neq 0 \\ 0 = (x \bmod p) & \text{if } x \bmod p = 0 \end{cases}$$

(by Little Fermat)

Thus $(x \bmod p)^{1+L} = x \bmod p$

Similarly: $(x \bmod q)^{1+L} = x \bmod q$

Together (CRT):

$$x^{1+L} = x \quad .$$

In particular:

Thm RSA is correct in all cases!

How to recognise a prime?

2012/10/11
brico
(20)

Observations:

- $\mathbb{Z}_m$ is a field $\iff$ m is prime.
- m is prime $\Rightarrow$ $x^{m-1} \equiv_m 1$ for any $0 < x < m$.
- if $\mathbb{Z}_m$ is a field then a degree 2 polynomial has at most 2 zeroes.
  In particular, there are at most two elements $1, -1$ such that $x^2 - 1 = 0$ in $\mathbb{Z}_m$.
- if p, q are primes then $x^2 - 1 = 0$ has four solutions over $\mathbb{Z}_{pq}$.

  Use CRT: $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$
  $\pm 1 \quad \pm 1$

  $1 \mapsto (1,1)$
  $? \mapsto (1,-1)$
  $? \mapsto (-1,1)$
  $-1 \mapsto (-1,-1)$

Now: the Fermat test does the following:

Given ℓ to check for primality.
Pick $a \in \mathbb{Z}_\ell \setminus \{0\}$.
If $a \notin \mathbb{Z}_\ell^\times$ then ℓ is not prime.
Compute $b = a^{\ell-1} \bmod \ell$.
If $b = 1$ then answer: ℓ may be prime.
If $b \neq 1$ then ℓ is not prime.

Strong Fermat test (Miller; Rabin)

Input: a number $\ell \in \mathbb{N}$

Output: a verdict: • ℓ is not prime
• ℓ may be prime

1. Pick $a \in \mathbb{Z}_\ell \setminus \{0\}$ at random.
2. If $a \notin \mathbb{Z}_\ell^\times$, i.e. $\gcd(a, \ell) \neq 1$ then ℓ is not prime
3. ~~Compute~~ Write $\ell - 1 = \lambda \cdot 2^s$, λ odd.
4. Compute $b_0 = a^\lambda$, $b_1 = a^{\lambda \cdot 2}$, $\vdots$, $b_s = a^{\lambda \cdot 2^s} = a^{\ell - 1}$ in $\mathbb{Z}_\ell$.
5. If $b_s \neq 1$ then ℓ is not prime.
6. If $b_0 = 1$ then ℓ may be prime.
7. Say $b_t \neq 1$, $b_{t+1} = 1$.
   If $b_t \neq -1$ then ℓ is not prime
8. Then answer: ℓ may be prime.

$O(k^3)$

Theorem

If ℓ is prime, ~~prob~~ then the alg. always ℓ may be prime.

If ℓ is not prime, then
the alg. says ℓ may be prime
with prob $\leq 1/4$.