Lecture Notes

Foundations of informatics — a bridging course
Mathematical tools

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Fall 2008

©2008 Michael Nüsken

Foundations of informatics — a bridging course
Fall 2008
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. $\boxed{2}$

(ii) Your room has 6 lamps, and the first and third are lit. $\boxed{3}$

(iii) Develop and describe a general procedure to escape. $\boxed{5}$

Exercise 1.2 (Cards dealt). (10 points)

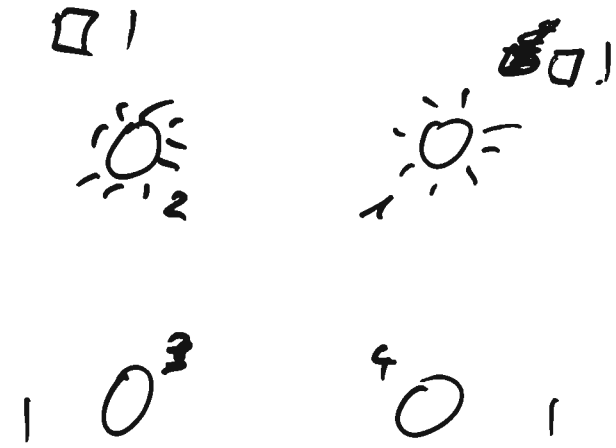
Consider a simple game: n players are sitting in a round. Player i has v_i cards. She may give $2k$ cards away, half to the left and half to the right. The team wins when finally all players have a multiple of m cards.

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 $v_1 = 2$, $v_2 = 3$, $v_4 = 7$. $\boxed{3}$

(ii) Say $n = 3$, $m = 5$, and $v_1 = 2$, $v_2 = 3$, $v_4 = 7$. $\boxed{3}$

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



bitwise addition modulo 2 (bitwise XOR)

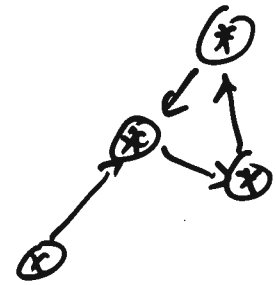
Input: $s = 1100$

① switch at 1 : 0001 $\quad + \; 1101 = a$

① at 2 : 1111 $\quad + \; 1110 = b$

⓪ at 3 $\quad + \; 0111$

⓪ at 4 $\quad + \; 1011$



Then $(s+a)+b = (s+b)+a$ "Order of switching does not matter."

Pf
- addition is commutative
  $a+b = b+a$
- addition is associative
  $(s+a)+b = s+(a+b)$

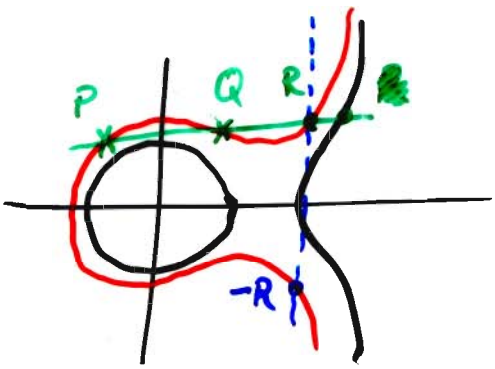
Putting this together ... □

Example for an associative operations

Consider an elliptic curve, $y^2 = x^3+ax+b$,

$\{(x,y) \in \mathbb{R}^2 \mid y^2 = x^3+ax+b\} \cup \{O\}$

not special in any sense



$P+Q := -R$

Is $(P+Q)+S = P+(Q+S)$?

Thm 2

We need every switch at most once in an optimal solution.

Pf Using a switch twice means to use a transition '+a' twice:

$$((s + a) + \dots) + a$$

$$= s + \underbrace{(a + a)}_{0} + \dots$$

$\square$

Output? • subset $\{1,2,3,4\}$.

• a vector of 4 bits.

In our example: 1100.

Our example: $s = 1100$

$$\begin{array}{cccc} & t & & \\ & 4 & & \\ + & 1 & \cdot & 1101 \\ + & 1 & \cdot & 1110 \\ + & 0 & \cdot & 0111 \\ + & 0 & \cdot & 1011 \\ \hline & & & 1111 \end{array}$$

transpose

multiplication modulo 2 (AND)

switch at 1

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{bmatrix} = \begin{bmatrix} 1 - s_1 \\ 1 - s_2 \\ 1 - s_3 \\ 1 - s_4 \end{bmatrix}$$

BriCo 3
14.10.08

Gaussian elimination

our problem

$$\begin{array}{c|cccc|c} (1) & 1 & 1 & 0 & 1 & 0 \\ (2) & 1 & 1 & 1 & 0 & 0 \\ (3) & 0 & 1 & 1 & 1 & 1 \\ (4) & 1 & 0 & 1 & 1 & 1 \end{array}$$

$$\begin{array}{c|cccc|c} (1') & 1 & 1 & 0 & 1 & 0 \\ (2') & 0 & 0 & 1 & 1 & 0 \\ (3') & 0 & 1 & 1 & 1 & 1 \\ (4') & 0 & 1 & 1 & 0 & 1 \end{array}$$

$= 1 \cdot (1)$
$= (2) - 1 \cdot (1)$
$= (3) - 0 \cdot (1)$
$= (4) - 1 \cdot (1)$

$$\begin{array}{c|cccc|c} (1'') & 1 & 1 & 0 & 1 & 0 \\ (2'') & 0 & 1 & 1 & 1 & 1 \\ (3'') & 0 & 0 & 1 & 1 & 0 \\ (4'') & 0 & 0 & 0 & 1 & 0 \end{array}$$

$= (1')$
$= 1 \cdot (3')$
$= (2') - 0 \cdot (2'')$
$= (4') - 1\ (2'')$

$$\begin{array}{c|cccc|c} (1''') & 1 & 1 & 0 & 1 & 0 \\ (2''') & 0 & 1 & 1 & 1 & 1 \\ (3''') & 0 & 0 & 1 & 1 & 0 \\ (4''') & 0 & 0 & 0 & 1 & 0 \end{array}$$

$= (4'')$
$= (2'')$
$= 1 \cdot (3'')$
$= (4'') - 0 \cdot (3''')$

$$\begin{array}{c|cccc|c} & 1 & 1 & 0 & 1 & 0 \\ & 0 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 1 & 1 & 0 \\ & 0 & 0 & 0 & 1 & 0 \end{array}$$

$= (4''')$
$= (2''')$
$= (3''')$
$= 1 \cdot (4''')$

$t_4 = 0$

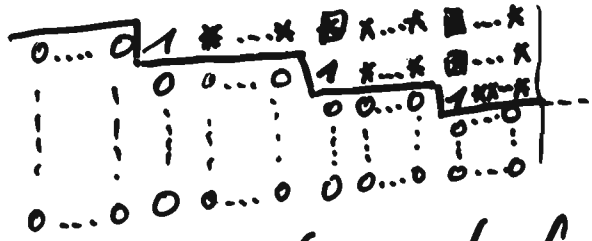
$t_3 = 0$

$t_2 = -t_3 - t_4 + 1 = 1$

$t_1 = -t_2 - t_4 + 0 = 1 + 0 + 0 = 1$

So: $t = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$.

Aim:

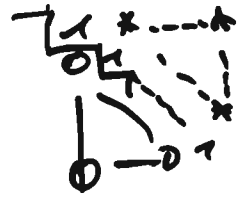


weak ~~triangular form~~ echelon

Allowed steps

- exchange rows
- multiply row by an invertible constant
- add a multiple of a row to another row.

"invertible" case: aim



Zri (d)
14.10.08

Gauß
- Jordan
- algorithm

$$\left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

$$\left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

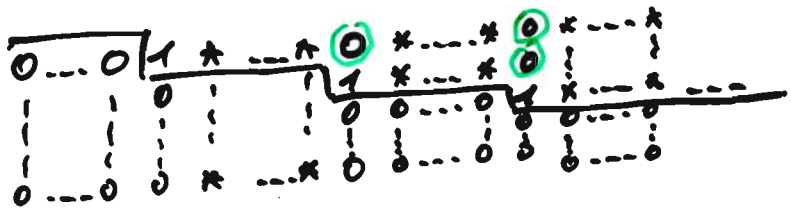
$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

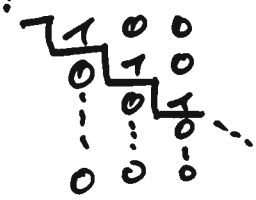
$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

← solution

Aim



"Invertible" case:



Allowed steps:
same as for
Gaussian elimination

Further questions:

- When do (no) solutions exist?
- How fast (slow) is this?
- Can we find the "inverse" matrix?
  ... and decide whether it exists?

How fast is Gaussian elimination
or Gauß-Jordan-algorithm?

Say we start with an $n \times n$ matrix.
then

$$O(n^3)$$ operations on elements

are enough.

⌈ V. Strassen 1971: Gaussian elimination is not optimal.

$$\rightarrow \quad O(n^{2.81}) = O(n^{\log_2 7})$$

by showing how to multiply 2x2-matrices (nicely) with only 7 multiplication

Best algorithm so far: $O(n^{2.38})$ Coppersmith & Winograd (1990)

Conjecture: $O(n^{2+\varepsilon})$. ⌋

<u>Proof</u>: For every of the n^2 element of the matrix we need at most one row operation which needs at most n elementary op's.

$$\rightarrow \quad n^2 \cdot O(n) \quad . \qquad \square$$

BriCo 6
14.10.08

Player 1's cards	Player 1's move	2's move	3's move
2	−2	1	1
3	+1	−2	1
	+1	1	−2

$$\begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

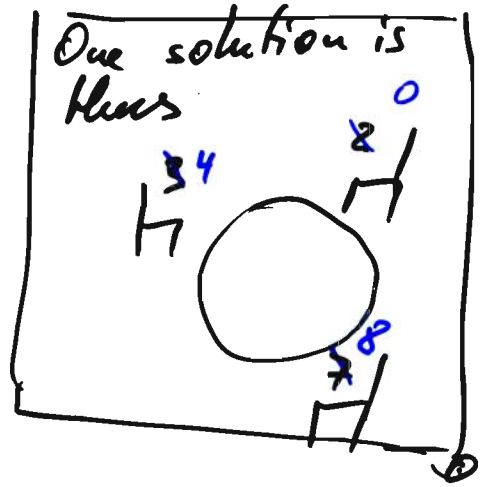
over "integers modulo m".

(i) We work modulo 4:

$$\begin{array}{c|ccc|c}
(1) & \boxed{-2} & 1 & 1 & -2 \\
(2) & 1 & -2 & 1 & -3 \\
(3) & \boxed{1} & 1 & -2 & -7 \\
\hline
(1') & 1 & \boxed{2} & 1 & 1 \\
(2') & 0 & 1 & 3 & 0 \\
(3') & 0 & \boxed{3} & 1 & 0 \\
\hline
(1'') & 1 & 0 & 3 & 1 \\
(2'') & 0 & 1 & 3 & 0 \\
(3'') & 0 & 0 & 0 & 0
\end{array}
\qquad
\begin{array}{l}
= 1\cdot(2) \\
= (1) - 2\,(1') \\
= (3) - 1\,(1') \\
= (1') - 2\,(2'') \\
= 1\cdot(2') \\
= (3') - 3\,(2'')
\end{array}$$

Note that: $-2 = 2$, $-3 = 1$, $-7 = 1$, $-1 = 3$ modulo 4 in $\mathbb{Z}_4$.

One solution is thus



$$\begin{aligned} k_1 + 3k_3 &= 1 \\ k_2 + 3k_3 &= 0 \\ 0 &= 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} k_1 &= k_3 + 1 \\ k_2 &= k_3 \end{aligned}$$

$$\rightarrow \left\{ \begin{bmatrix} k_3+1 \\ k_3 \\ k_3 \end{bmatrix} ; \; k_3 \in \mathbb{Z}_4 \right\} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix} \right\}$$

Expansion

$$\begin{array}{c|ccc|c}
 & 1 & 0 & 3 & 1 \\
 & 0 & 1 & 3 & 0 \\
\text{new row:} & 0 & 0 & -1 & 0
\end{array}$$

all solutions:

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + (-k_3) \begin{bmatrix} 3 \\ 3 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 + k_3 \\ k_3 \\ k_3 \end{bmatrix}$$

⚠ 4 is not prime.
$\mathbb{Z}_4$ is not a field.

Assume Gauß-Jordan yields

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

Expansion

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

All solutions:

$$\begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 3 \\ 0 \end{bmatrix} + \alpha \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \delta \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

Another example: assume Gauß-Jordan yields

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

NO SOLUTION.
(DO NOT EXPAND.)

Bri (8)
14.00.08

Over $\mathbb{Z}_p$ with p prime
no problems occur
since • $\mathbb{Z}_p$ is a field
i.e. every number but 0
is invertible.

We'll make more precise later.

How do sets of all solutions of linear systems look like?

We start with an equation

$$A \cdot x = b \quad \text{over } F \text{ a field.}$$

$$A \in F^{m \times n}, \; b \in F^m.$$

(e.g. $F = \mathbb{R}$, $F = \mathbb{C}$, $F = \mathbb{Q}$, $F = \mathbb{Z}_2$, $F = \mathbb{Z}_5$, $F = \mathbb{Z}_7$, ...)

We consider

$$S = \{ x_1 \in F^n \mid A x_1 = b \}$$

Whatever we do we easily see

"kernel of A"

$$S = x_0 + \underbrace{\{ x \in F^n \mid Ax = 0 \}}_{=: \ker A}$$

provided $A x_0 = b$.

Proof: Given $x_1 \in S$. Then $A x_1 = b$. So $A(x_1 - x_0) = b - b = 0$.
Thus $x_1 = x_0 + \underbrace{(x_1 - x_0)}_{\in \ker A}$, i.e. $x_1 \in x_0 + \ker A$.
Conversely, given $x_0 + x$ with $Ax = 0$. Then $A(x_0 + x) = b + 0 = b$. $\square$

Size of $\ker A$?

Or better: $\dim \ker A = ?$

<u>Thm</u>

$$\dim \ker A + \underbrace{\dim \operatorname{range} A}_{\operatorname{rank} A} = n.$$

?

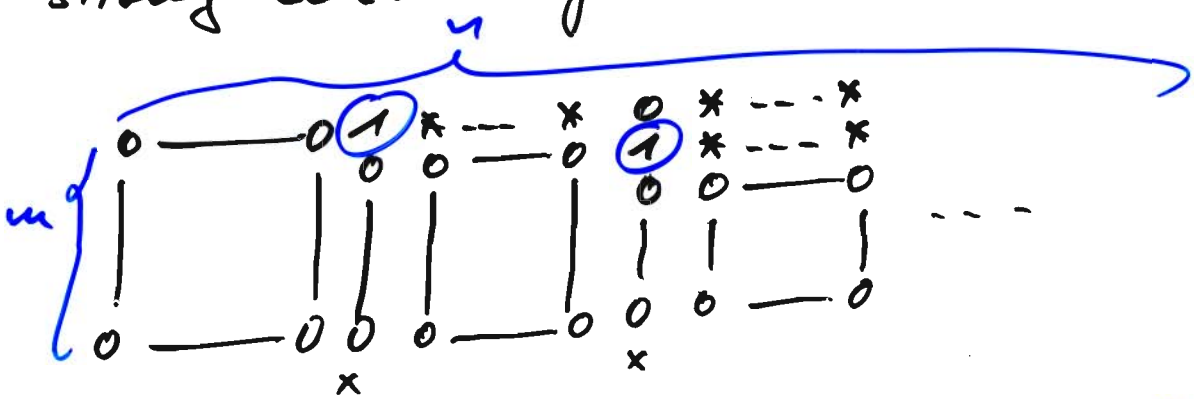
~~After~~

Notice: Gauß-Jordan-algorithm

(a) does not change the space of solutions.

(b) does not change the rank of the matrix (but it does change the range of the matrix)

After Gauß-Jordan we have strong echelon form:



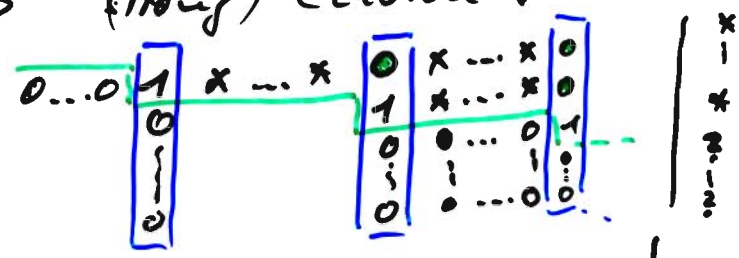
# of these special 1's = rank A.

$\dim \ker A$ = # non 1' columns

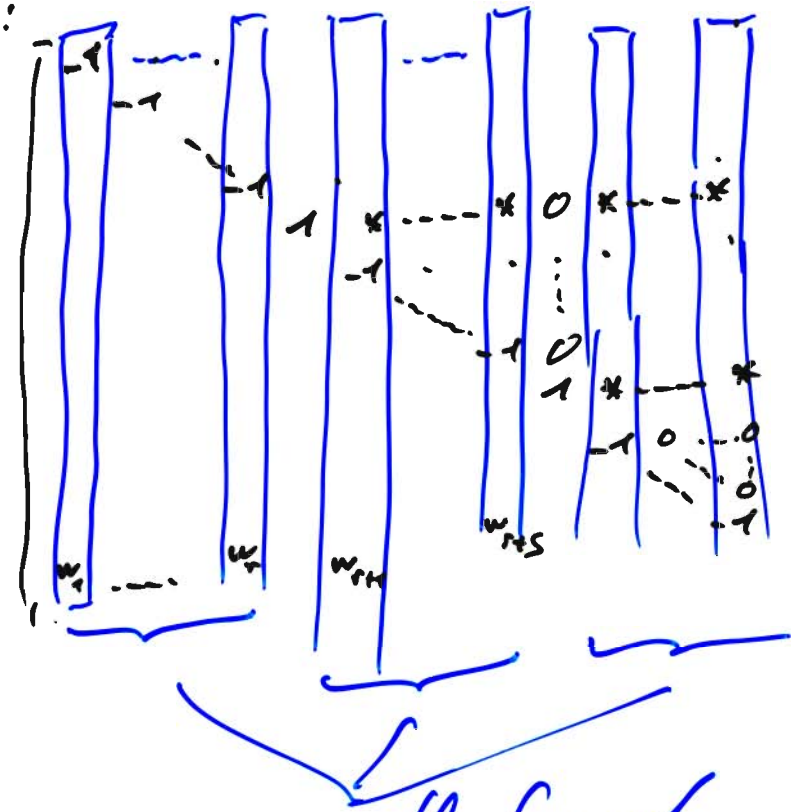
Summary

- Gaussian elimination (numerically more stable)
- Gauß-Jordan-algorithm (nicer result)
- Expansion
- $\ker A = \{ x \mid Ax = 0 \}$

Gauß-Jordan $\rightsquigarrow$ (strong) echelon form



unless there is a zero row with nonzero rhs you expand:



span the kernel

$$\ker A = \{ \sum_i \alpha_i \cdot w_i \mid \alpha_i \in F \}$$

- $\ker A$ is a vector space.

  $\operatorname{range} A$ is also a vector space.

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

  $$Ax = \sum_{i=1}^{n} x_i \underbrace{A_{\cdot i}}_{i\text{-th column of } A}.$$

- To obtain a <u>basis</u>

  for $\ker A$: run Gauß-Jordan and expand

  then the "-1"-vectors are a basis of the kernel.

  for $\operatorname{range} A$: pick those columns in A where you have the "1"-columns in the transformed matrix, they form a basis of the range.

Obvious now: $\underbrace{\dim \ker A}_{\text{defect } A} + \underbrace{\dim \operatorname{range} A}_{\text{rank } A} = n$

Looking more closely.

We can describe each row operation as a multiplication with a certain matrix:

- swap row i and row j

$$
\begin{array}{c}
\\ \\ i \\ \\ \\ \\ \\
\end{array}
\begin{bmatrix}
1 & & & & & & & & \\
 & \ddots & & & & & & & \\
 & & 1 & & & & & & \\
 & & & 0 & & & & 1 & \\
 & & & & 1 & & & & \\
 & & & & & \ddots & & & \\
 & & & & & & 1 & & \\
 & & 1 & & & & & 0 & \\
 & & & & & & & & 1 \\
 & & & & & & & & & \ddots \\
 & & & & & & & & & & 1
\end{bmatrix}
$$

This matrix is square and <u>invertible</u>.

- multiple ~~a~~ row i by an invertible constant α

$$
\begin{array}{c}
\\ \\ i \\ \\ \\
\end{array}
\begin{bmatrix}
1 & & & & & \\
 & \ddots & & & & \\
 & & 1 & & & \\
 & & & \alpha & & \\
 & & & & 1 & \\
 & & & & & \ddots \\
 & & & & & & 1
\end{bmatrix}
$$

This matrix is square and <u>invertible</u>.

- add ~~row i to~~ multiples of row i to other rows

$$
\begin{array}{c}
\\ \\ i \\ \\ \\ \\ \\
\end{array}
\begin{bmatrix}
1 & & & * & & & \\
 & \ddots & & \vdots & & & \\
 & & 1 & * & & & \\
 & & & 1 & & & \\
 & & & * & 1 & & \\
 & & & \vdots & & \ddots & \\
 & & & * & & & 1
\end{bmatrix}
$$

This matrix is square and <u>invertible</u>.

Now each transition in the Gauß-Jordan-algorithm is of the form:

$$A'x = b' \xrightarrow[\text{by } M]{\text{multiply}} MA'x = Mb'.$$

The entire algorithm transforms

$$Ax = b$$

into

$$(M_T M_{T-1} \cdots M_1) A x = (M_T M_{T-1} \cdots M_1) b .$$

each of these is one of the above row operation matrices, in particular, each is <u>invertible</u>

So this product also is invertible.

<u>Theorem</u> For every matrix A (and vector b) there exists an invertible matrix M such that (i) MA is in strong echelon form

(ii) MA is in weak echelon form (ie. upper triangular)

and * up to a permutation of rows M is lower triangular.

We can rewrite

$$PA = L \cdot R$$

product of transforms.

M^{-1}

transformed PA. = transformed A

Bri (6.14)
15.10.08

Using L·R decomposition is helpful when solving for many or only later known rhs-s b:

$$Ax = b \,?$$

given $PA = LR$ i.e.

$$LRx = PAx = Pb.$$

Solving is now a two-step substitution/back-substitution:

$$Ly = Pb$$

$\cdot y = Pb$

$y_1 \leftarrow l_{11} y_1 = (Pb)_1$

$l_{21} y_1 + l_{22} y_2 = (Pb)_2$

"substitution"

and

$$Rx = y$$

$r_{nn} x_n = y_n$

$r_{n-1,n-1} x_{n-1} + r_{n-1,n} x_n = y_{n-1}$

"back substitution"

So knowing the L-R-decomposition it takes only $O(n^2)$ time to solve $Ax = b$?

- How to compute M easily?
- How to compute A^{-1}?
- What is the strong echelon form of an invertible matrix?

Assume A is invertible.

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

$= \{ x \mid BAx = 0 \}$

for any invertible B

using $B = A^{-1}$ yields:

$= \{ x \mid x = 0 \}$

thus $\dim \ker A = 0$.

and $\operatorname{rank} A = n$.

Now, the only rank n strong echelon form matrix is

$$\begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ \vdots & 0 & \ddots & \\ \vdots & \vdots & & \\ \vdots & \vdots & & \\ 0 & 0 & & 1 \end{bmatrix}.$$

So we need the M that the Gauß-Jordan-Algorithm uses: $M = A^{-1}$.

~~Note that $A^{-1}A =$~~

Q: How to easily solve $Ax_1 = b$ and $Ax_2 = c$ simultaneously?

Put $A \mid b\, c$ in the tableau and run Gauß-Jordan.

So do that for all unit vectors simultaneously:

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

Then Gauß-Jordan gives

$$MA \mid \underbrace{M\mathbb{1}}_{M}.$$

So this is how we get M easily and if A is invertible then $MA = \mathbb{1}$ (because it is strong echelon form of rank n) so $A^{-1} = M$.

<u>Example</u>

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{over} \quad \mathbb{Z}_7$$

$$b = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \quad c = \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}, \quad \cancel{A^{-1} = ?}$$

$$Ax = b, \quad Ay = c, \quad A^{-1} = ?$$

$$\begin{array}{c|ccc|cc|ccc}
\mathbb{1} & 1 & 2 & 3 & 1 & 3 & 1 & 0 & 0 \\
\mathbb{1} & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\
 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 1 \\
\hline
 & 1 & 0 & 3 & 4 & 3 & 1 & 5 & 0 \\
 & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\
\mathbb{2} & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 1 \\
\hline
\downarrow & 1 & 0 & 0 & 4 & 5 & 1 & 5 & 2 \\
\det A = 2 & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\
 & 0 & 0 & 1 & 0 & 4 & 0 & 0 & 4
\end{array}$$

$1 \cdot 4$

DONE

$$x = \begin{bmatrix} 4 \\ 2 \\ 0 \end{bmatrix}, \quad y = \begin{bmatrix} 5 \\ 0 \\ 4 \end{bmatrix},$$

$\ker A = \{0\}$

$\operatorname{range} A = \left\langle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \\ 2 \end{bmatrix} \right\rangle$

in particular A^{-1} exists and

$$A^{-1} = \begin{bmatrix} 1 & 5 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}.$$

Foundations of informatics — a bridging course
Fall 2008
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:

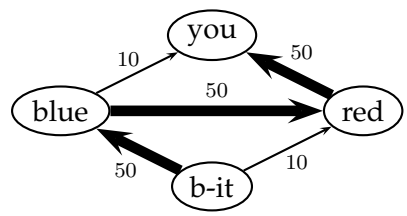


Figure 2.1: Network

(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, $t_{\text{b-it,blue}} + t_{\text{blue,you}} =$ 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.

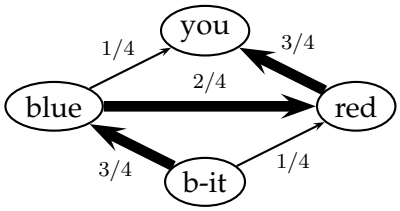


Figure 2.2: Relative flows

Exercise 2.1. (10 points)

(i) Set up a system of linear equations describing the entire system. $\boxed{4}$

(ii) Solve it and read off the flows. $\boxed{4}$

(iii) Determine the complete flow f. $\boxed{2}$

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

Missing: Determinant.

BriCo 17
15.10.08

<u>Def</u> Given $A \in F^{n \times n}$ square.

Then
- $\det A = \prod$ diagonal elements if A is in triangular form.
- $\det(A \cdot B) = \det A \cdot \det B$
- $\det\left(\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & 1 \end{bmatrix}\right) = -1.$

By the L-R-decomposition this defines the determinant.

To compute it, just execute Gaussian elimination or Gauß-Jordan-algorithm and ~~write~~ note for ● a -1 and for ● the α^{-1}. If then at the end we do not have a non "1"-column, then $\det A$ = product of the noted values. (the -1's and $(\alpha)^{-1}$'s)

Otherwise $\det A = 0$.

Another definition:

$$\det A = \sum_{\substack{\pi \text{ permutations} \\ \text{of } n \text{ elements}}} (-1)^{\operatorname{sign}(\pi)} A_{1\pi(1)} \cdot \ldots \cdot A_{n\pi(n)}$$

Using this the calculation costs $O(n! \cdot n) \gg O(2^n)$ so using Gaussian elimination is MUCH cheaper: $O(n^3)$.

Foundations of informatics — a bridging course
Fall 2008
Mathematical tools

MICHAEL NÜSKEN

3. Probabilities

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

Give examples where randomness

(i) decides about win or loose. $\boxed{2}$

(ii) helps simulating difficult reality. $\boxed{2}$

(iii) helps solving difficult finite problems. $\boxed{2}$

(iv) models errors. $\boxed{2}$

(v) makes decisions. $\boxed{2}$

(vi) hides secrets. $\boxed{2}$

(vii) Does something else which is interesting. $\boxed{+4}$

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? $\boxed{5}$

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. $\boxed{2}$

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

5 What do you do? Reason!

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!]

?

Probabilities

BnYo (18)
15.0.08

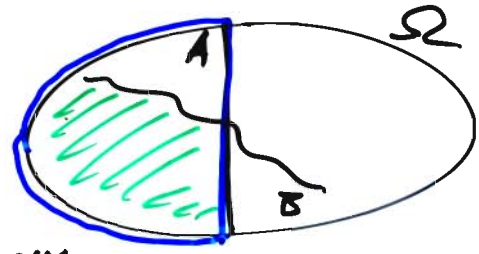
...of events

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

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

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

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



Conditional probility:

Given that A occured, what is the probability for B now.

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

Example: die
$A = \{2,4,6\}$
$B = \{4,5,6\}$
$\text{prob}\,B = 1/2$
$\text{prob}(B|A) = \frac{2}{3}$

A and B are <u>independent</u> iff $\text{prob}(A \cap B) = \text{prob}A \cdot \text{prob}B$.

...of random variables

A random variable tells 'the outcome' of an experiment. We use events like

$$A_i = \{ \text{COIN}_i = \text{heads} \}$$

and assume $\text{prob}(\text{COIN}_i = \text{heads}) = \frac{1}{2}$, say.

Then $\text{prob}(\text{COIN}_1 = \text{heads} \wedge \text{COIN}_2 = \text{heads})$

$= \frac{1}{2} \cdot \frac{1}{2}$ <u>assuming</u> that the r.v. COIN_1, COIN_2 are independent.

Many r.v. output real numbers like

$X_i = 1$ if ~~we can exit after hour i.~~ prisoner i says YES, I go.

$\sum_{i=1}^{100} X_i$ then describes the number of prisoners saying YES...

Two r.v. X, Y are <u>independent</u> iff $\forall x, y$:

Bri 6 (19)
15.10.08

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

Prisoner's dilemma:

Strategy p:
- Input: Nothing
- Output: ~~YES or NO~~ 1 or 0.
  1. Roll a coin that comes up heads with probability p.
  2. RETURN $\begin{cases} 1 & \text{if it came up heads} \\ 0 & \text{otherwise.} \end{cases}$

Let $P_i = 1$ iff Prisoner i says YES.

Assume $\text{prob}(P_i = 1) = p$,
$\text{prob}(P_i = 0) = 1 - p$,

and assume that all these 100 r.v. are independent.

Bri(o 20
15.10.08

Number of prisoners that choose to go:

$$X = \sum_{i=1}^{100} X_i$$

Number of prisoners that are allowed to go:

$$Y := \begin{cases} X & \text{if } X < 100, \\ 0 & \text{if } X = 100. \end{cases}$$

$$\text{prob}(X=0) = \text{prob}(X_1=0 \wedge X_2=0 \wedge X_3=0 \wedge \ldots \wedge X_{100}=0)$$
$$= (1-p)^{100}$$

$$\text{prob}(X=i) = \binom{100}{i} p^i (1-p)^{100-i}$$

$$\ulcorner = \text{prob}\Big(\exists S \in \binom{1..100}{i} : \underbrace{X_i := \begin{cases} 1 & i \in S \\ 0 & i \notin S \end{cases}}_{S = \{i \mid X_i = 1\}}\Big)$$

$$= \underbrace{\sum_{S \in \binom{1..100}{i}}}_{= \binom{100}{i}} \underbrace{\text{prob}(S = \{i \mid X_i = 1\})}_{p^i (1-p)^{100-i}} \quad = \text{daiman} \lrcorner$$

Want: the expected number of participants:

$$E(Y) = \sum_{y \in 0,\ldots,100} \text{prob}(Y=y) \cdot y$$

Bin'Co (24)
15.10.08

$$= \sum_{y=0}^{99} \text{prob}(X=y) \cdot y$$

$$+ \text{prob}(X=100) \cdot 0$$

$$= \sum_{y=0}^{99} \binom{100}{y} p^{y} (1-p)^{100-y} \cdot y$$

$$= \underbrace{\sum_{y=0}^{100} \text{----}}_{?} - p^{100} \cdot 100 .$$

$$x = \frac{p}{1-p}$$

$$\sum_{i=0}^{100} \binom{100}{i} x^{i} \cdot i =$$

$$\frac{d}{dx} : (1+x)^{100} = \sum_{i=0}^{100} \binom{100}{i} x^{i}$$

$$\cdot x : 100 (1+x)^{99} = \sum_{i=0}^{100} \binom{100}{i} i x^{i-1}$$

$$100 x (1+x)^{99} = \sum_{i=0}^{100} \binom{100}{i} i x^{i} .$$

$$= (1-p)^{100} 100 \frac{p}{1-p} \underbrace{\left(1 + \frac{p}{1-p}\right)}_{\frac{1}{1-p}}^{99} - 100 p^{100} .$$

$$= 100 p - 100 p^{100} .$$

$$= 100 p (1 - p^{99})$$

Find p that maximizes this.

BriCo ㉒
15.10.08

Pollard-ρ

Input: a number N, (which is not prime)

Output: a proper factor a of N.

Fix a function $f: \mathbb{Z}_N \to \mathbb{Z}_N$

$\shortparallel$ $\{0,1,2,\dots N-1\}$.

e.g. $f(x) = x^2+1$.

Compute $x_0 \in_R \mathbb{Z}_N$,

$x_1 = f(x_0)$,

$x_2 = f(x_1)$

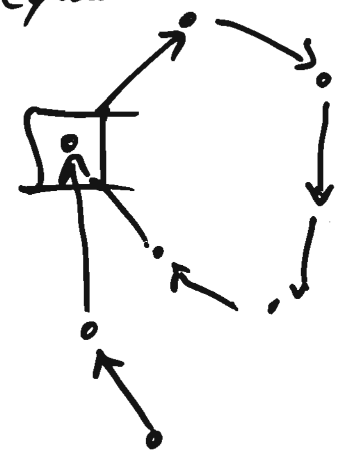
$\vdots$

until $\exists i<n$: $\gcd(x_n - x_i, N) \neq 1$.

Return $\gcd(x_n - x_i, N)$ unless it's equal N, else FAIL.

Now: assume $p \mid N$

then $\left.\begin{array}{l} x_0 \bmod p \\ x_1 \bmod p \\ \vdots \end{array}\right\}$ in $\mathbb{Z}_p$



prob(exit after n steps)

$\approx 1 - \left(1 - \frac{1}{t}\right)^n \approx \frac{n}{t}$

↑ for small n

$E(\#\text{ of iterations}) \approx \sqrt{t}$.

$t \le \sqrt{N}$.

runtime $\approx \sqrt[4]{N}$

Random exit

$X_i = 1$ iff exit at step i

$N = i \quad :\Longleftrightarrow \quad X_i = 1.$

$N = \min\{i \mid X_i = 1\}.$

$= i \quad : \quad X_0 = 0, \dots, X_{i-1} = 0, \; X_i = 1.$

$$E(N) = \sum_{i \geq 1} \underbrace{\text{prob}(N=i)}_{= (1-p)^{i-1} \cdot p} \cdot i$$

if $\text{prob}(X_i = 1) = p$, and all X_i are independent

$$= p \underbrace{\sum_{i \geq 1} (1-p)^{i-1} i}$$

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

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

$$\sum_{i \geq 1} i \cdot q^{i-1} = \frac{1}{(1-q)^2}$$

$$\sum_{i \geq 0} q^i = \frac{1}{1-q} \quad \text{for } |q| < 1.$$

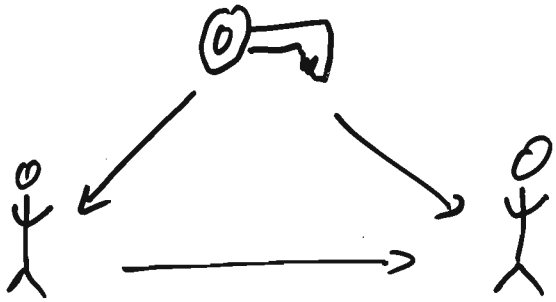
$$\frac{d}{dq}: \quad \sum_{i \geq 0} i q^{i-1} = \frac{+1}{(1-q)^2}$$

Thus we expect

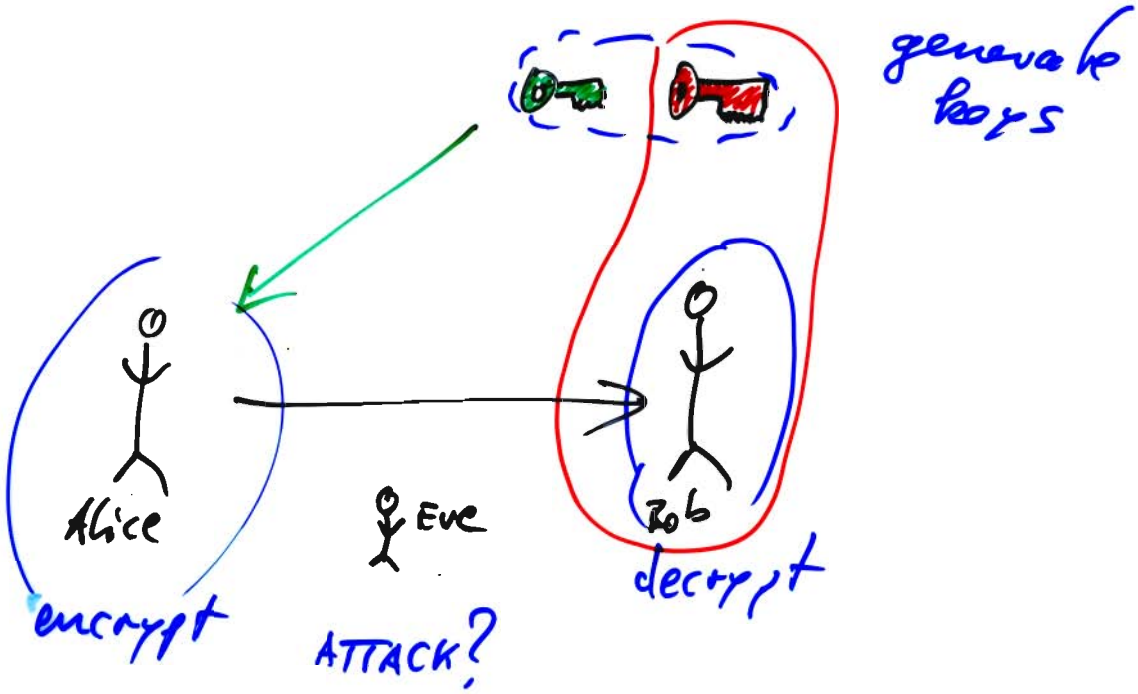
$\frac{1}{p}$ iterations till exit.

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \quad \Big/ \quad \binom{\{1,\dots,n\}}{i}$$

Classically:



New solution: [1970-72 British Secret Service]
1976 Diffie & Hellman
1978 Rivest, Shamir, Adleman



RSA

generate keys

Input: n a security parameter

Output: key pair random!

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

encrypt

Input: public key (N, e), message $x \in \mathbb{Z}_N = \{0, 1, \dots, N-1\}$ $O(n^3)$

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

1. Compute $y := x^e$ in $\mathbb{Z}_N$.

decrypt

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

Output: message $z \in \mathbb{Z}_N$ $O(n^3)$

1. Return $z := y^d$ in $\mathbb{Z}_N$.

To Do:

(0) Understand the program.

(1) Correctness:
Prove that $z = x$!

(2) Efficiency:
Prove that everything can be done fast.

(3) Security:
?

First: <u>integers modulo N</u>

We know: integers $\mathbb{Z}$
and its' operations: $+$ addition,
$\cdot$ multiplication,
$-$ negative,
0 zero,
1 one,
(? powering ....)

Let N be any integer, $N \geq 2$.
Define integers modulo N.

division with remainder

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$$ elements (of our new class)

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

where:

Thm Division with remainder works: $y \neq 0$
given $x, y \in \mathbb{Z}$ then there exists $q, r \in \mathbb{Z}$ such that

$$x = q \cdot y + r \wedge 0 \leq r < |y|.$$

Example
$(5 \text{ rem } 7) + (5 \text{ rem } 7)$
$= 5 +_{\mathbb{Z}} 5 = 10.$
$(5 \bmod 7) + (5 \bmod 7)$
$= 5 +_{\mathbb{Z}_7} 5 = 3.$

Def $r =: x \text{ rem } y \in \mathbb{Z}$,
$q =: x \text{ quo } y \in \mathbb{Z}$,
$\mathbb{Z}_N(r) =: x \bmod y \in \mathbb{Z}_y$.

So addition now is well def'd.

$$a \cdot_{\mathbb{Z}_N} b := (a \cdot_{\mathbb{Z}} b) \bmod N \in \mathbb{Z}_N$$

<u>Thm</u> $(\mathbb{Z}_N, +_{\mathbb{Z}_N}, \cdot_{\mathbb{Z}_N})$ is a <u>commutative ring</u>.

<u>Pf</u>

P+ : Addition is well def'd (proper)

That's true by construction.

A+ : $(a+b)+c = a+(b+c)$

$$\begin{aligned}(a+b)+c &= ((a +_{\mathbb{Z}} b \bmod N) +_{\mathbb{Z}} c) \bmod N \\ &= ((a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c) \bmod N \\ &= (a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c)) \bmod N \\ &= a+(b+c) \quad \checkmark\end{aligned}$$

N+ : $a + 0 = a = 0 + a$

$0 := 0 \bmod N$.

I+ : $\forall a \exists b$: $a + b = 0 = b + a$

$a \in \mathbb{Z}_N$. Then: $b := (\underset{\mathbb{Z}\text{-negative}}{-a}) \bmod N$.

C+ : $a+b = b+a$.

$$\begin{aligned}a+b &= (a +_{\mathbb{Z}} b) \bmod N = (b +_{\mathbb{Z}} a) \bmod N \\ &= b+a.\end{aligned}$$

P.: Multiplication is well def'd

That's true by definition.

A.: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$\ulcorner$ $(a \cdot b) \cdot c = (((a \cdot_{\mathbb{Z}} b) \operatorname{rem} N) \cdot_{\mathbb{Z}} c) \bmod N$

Write: $a \cdot b = q \cdot N + r$, $0 \le r < N$.
ie. $a \cdot b \operatorname{rem} N = r$
$= ab - qN$

$\ldots = \overset{\exists q \in \mathbb{Z}}{=} (((a \cdot_{\mathbb{Z}} b) -_{\mathbb{Z}} q \cdot_{\mathbb{Z}} N) \cdot_{\mathbb{Z}} c) \bmod N$

$= ((a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c -_{\mathbb{Z}} \underbrace{q \cdot_{\mathbb{Z}} c \cdot_{\mathbb{Z}} N}_{\% \bmod N = 0 \bmod N}) \bmod N$

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

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

$\ldots = a \cdot (b \cdot c)$. ✓ $\lrcorner$

N.: $a \cdot 1 = a = 1 \cdot a$

Yes: $1 = 1 \bmod N$.

(I.: ? Not always, see below.)

C.: $a \cdot b = b \cdot a$ ✓

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

$\ulcorner$ similar to A. $\lrcorner$

ON'T: $0 \neq 1$. (Since $N \geq 2$.) $\square$

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

Well, by definition:

$$x^e = \underbrace{(\cdots((((x \cdot_{\mathbb{Z}_N} x) \cdot_{\mathbb{Z}_N} x) \cdot_{\mathbb{Z}_N} x) \cdot_{\mathbb{Z}_N} x) \cdot_{\mathbb{Z}_N} \cdots) \cdot_{\mathbb{Z}_N} x}_{\substack{e \text{ factors.} \\ e-1 \text{ products.}}}$$

That's much too slow, since our $e \approx 2^{1024}$.

The age of the universe: 2^{150} Planck units.

Well ☹

Idea: $x^e = ((x \cdot x) \cdot (x \cdot x)) \cdot ((x \cdot x) \cdot (x \cdot x)) \cdots$

$= ((x^2)^2)^2 \cdots$

Make it precise: $x^{42} = x^{101010_2}$

$10_2 \cdot 10_2 = 100_2$

$$= \underbrace{(((\underbrace{(x^{10_2})^{10_2}}_{x^{101_2}} \cdot_{\mathbb{Z}_N} x)^{10_2})^{10_2} \cdot_{\mathbb{Z}_N} x)^{10_2}}_{x^{101010_2}}$$

Here we need: 5 squarings
and 2 multiplications.

Ie: 7 multiplications
instead of 41 in the first
approach.

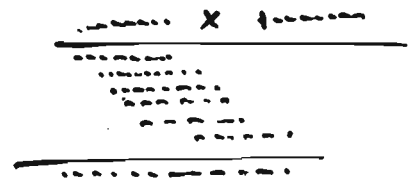
This is called Square-and-Multiply

Bri(d30)
16.10.08

<u>Exercise</u>: Write an algorithm with input x, e and output x^e.

<u>Thm</u> With S&M we need at most $n-1$ squarings and $n-1$ multiplications (for an n-bit exponent), i.e. $O(n)$ operations in the domain of x.

For RSA $n = \text{bitlength}(N)$ and an operation is a multiplication in $\mathbb{Z}_N$ which costs $O(n^2)$ bit operations.



Actually, we can do better:

Schönhage & Strassen (≈1970): $O(n \log n \log\log n)$

Fürer (2007): $O(n \log n \, \underbrace{2^{\log^* n}}_{\text{in practice } \leq 32})$

Karatsuba (≈1960): $O(n^{\underbrace{\log_2 3}_{\approx 1.57}})$

$$(a_1 t + a_0)(b_1 t + b_0) = a_1 b_1 t^2 + (a_1 b_0 + a_0 b_1) t + a_0 b_0$$

$$\| $$

$$p_2 t^2 + (p_1 - p_2 - p_3) t + p_3$$

Take $t = 2^{n/2}$ and $0 \leq a_0, b_0 < t$

Compute: $p_1 := (a_1 + a_0) \cdot (b_1 + b_0)$

$p_2 := a_1 b_1$

$p_3 := a_0 b_0$

So we can do with 3 half length products.

Back to RSA:

x^e in $\mathbb{Z}_N$ can be done

in at most $\underbrace{O(n) \cdot O(n^2)}_{O(n^3)}$ bit operations

(With fast arithmetics: $O(n^2 \log n \log\log n)$)

<u>Corollary</u>

Encrypt & decrypt in RSA in $O(n^3)$ time. $\square$

Next question: how to find $e, d \in \mathbb{Z}$ such that

$$e \cdot d = 1 + k \cdot L \quad \text{for some } k \in \mathbb{Z} \,?$$

That is, how to find $e, d \in \mathbb{Z}_L$ such that

$$e \cdot d = 1 \,?$$

So this is a question about finding inverses in a ring of integers modulo L.

Say, we are given $e \in \mathbb{Z}_L$

How to decide whether the inverse exists and then to find it ?

Ie: How to find d such that $ed = 1$ in $\mathbb{Z}_L$?

How to find d and k such that

$$de - kL = 1 \quad \text{in } \mathbb{Z} \,?$$

Observation: 1 is a very small positive integer.

So instead of trying to directly find a solution, try to have a not too bad start and find a way to improve it!

Eg: $d=1, -k=0$ gives $1\cdot e - 0\cdot L = e$ (1)

or $d=0, -k=1$ gives $0\cdot e + 1\cdot L = L$ (2)

Make it better:

maybe the difference: $-1\cdot e + 1\cdot L = L-e > 0$

or subtracting (1) twice $-2\cdot e + 1\cdot L = L-2e$ –?

! subtract as often as possible: (2) $- q\cdot$(1): $-q\cdot e + 1\cdot L = \underset{r}{\underset{\shortparallel}{L-qe}}$

$L = q\cdot e + r$

with $0 \le r < e$

(div. with remainder)

This leads to the

Extended Euclidean Algorithm

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

$e = 35$

Bri(d) 33
16.10.08

i	r_i	q_i	s_i	t_i	remarks
0	$L=60$		1	0	$60 = 1\cdot 60 + 0\cdot 35$
1	$e=35$	$\boxed{1}$	0	1	$35 = 0\cdot 60 + 1\cdot 35$
2	25	$\boxed{1}$	1	-1	$25 = 1\cdot 60 - 1\cdot 35$
3	10	$\boxed{2}$	-1	2	$10 = -1\cdot 60 + 2\cdot 35$
4	5	$\boxed{2}$	3	-5	$5 = 3\cdot 60 - 5\cdot 35$
5	0 (STOP)		-7	12	$0 = -7\cdot 60 + 12\cdot 35$

$60 = \boxed{1}\cdot 35 + \boxed{25}$
$35 = \boxed{1}\cdot 25 + \boxed{10}$
$25 = \boxed{2}\cdot 10 + 5$
$10 = \boxed{2}\cdot 5 + 0$

$7 = \frac{35}{5}$, $12 = \frac{60}{5}$

5 divides $L=60$
5 divides $e=35$ $\Big\} \Rightarrow 5 \mid (s\cdot L + te)$ for any $s,t \in \mathbb{Z}$

but $5 \nmid 1$

Thus there cannot exist a solution of $s\cdot L + t\cdot e = 1$.

Let's try another e:

$L=60$, $e=13$.

i	r_i	q_i	s_i	t_i	remarks
0	$L=60$		1	0	$60 = 1\cdot 60 + 0\cdot 13$
1	$e=13$	$\boxed{4}$	0	1	$13 = 0\cdot 60 + 1\cdot 13$
2	8	1	1	-4	$8 = 1\cdot 60 - 4\cdot 13$
3	5	1	-1	5	$5 = -1\cdot 60 + 5\cdot 13$
4	3	1	2	-9	
5	2	1	-3	14	
6	1	2	5	-23	our solution!
7	0		-13	60	our cross check! $0 = -13\cdot 60 + 60\cdot 13$ obviously ok.

$60 = \boxed{4}\cdot 13 + 8$, $0 < 8 < 13$
$13 = 1\cdot 8 + 5$
$8 = 1\cdot 5 + 3$

Thus (0) crosscheck ok.

(1) $1 = 5 \cdot 60 + (-23) \cdot 13$ in $\mathbb{Z}$

(2) $1 = (-23) \cdot 13$ in $\mathbb{Z}_{60}$

or $1 = 37 \cdot 13$ in $\mathbb{Z}_{60}$

Thus $13^{-1} = 37$ in $\mathbb{Z}_{60}$.

<u>Exercise</u>

- Calculate 15^{-1} in $\mathbb{Z}_{53}$.

$13 \cdot 53$: 520, 159; 460, 230, 690

$46 \cdot 15 = 1$ ✓

- Calculate 15^{-1} in $\mathbb{Z}_{90}$. No solution, 5 | 15 and 5 | 90; because of this every combination ... is divisible by 5 but 1 is not.
- Calculate 7^{-1} in $\mathbb{Z}_{401}$. $7 \cdot 29 = 1$.

<u>Solution to Exercise</u> Write down the algorithm for square & multiply:

S&M

Input: x an element from some domain which allows multiplication (assoc, neutral)

e a natural number.

Output: x^e.

1. Let $(e_{n-1}, e_{n-2}, e_{n-3}, \ldots, e_1, e_0)$ be the binary representation of e. ($e_{n-1} = 1$)
2. $y := x$ (of the domain containing x).
3. FOR i from $n-2$ to 0 do
4. $\quad y := y^2$.
5. $\quad$ IF $e_i = 1$ THEN $y := y \cdot x$.
6. Return y.

Brilo (35)
16.10.08

EEA

Input: a, b
→ length ℓ and
Output: → Tableau or
→ Last but one line

1. $r_0 := a$, $s_0 := 1$, $t_0 := 0$.
2. $r_1 := b$, $s_1 := 0$, $t_1 := 1$.
3. $i := 1$, WHILE $r_i \neq 0$ DO
4. divide r_{i-1} by r_i with remainder so that
   $$r_{i-1} = q_i \cdot r_i + r_{i+1}$$
   and $0 \leq r_{i+1} < |r_i|$.
4a. $r_{i+1} = r_{i-1} - q_i r_i$ (assertion).
5. $s_{i+1} := s_{i-1} - q_i s_i$.
6. $t_{i+1} := t_{i-1} - q_i t_i$.
7. Increase i
8. END
9. Return $(i-1, r_{i-1}, s_{i-1}, t_{i-1})$

$$\begin{array}{cccc} \overset{\shortparallel}{i-1} & \overset{\shortparallel}{r_{i-1}} & \overset{\shortparallel}{s_{i-1}} & \overset{\shortparallel}{t_{i-1}} \\ \overset{\shortparallel}{\ell} & \overset{\shortparallel}{r_\ell} & \overset{\shortparallel}{s_\ell} & \overset{\shortparallel}{t_\ell} \end{array}$$

Thm

(i) $r_i = s_i a + t_i b$.

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

(iii) $\ell < \infty$, $\ell \in O(n)$

$\uparrow$ bitlength of a or b whatever is larger.

Actually, with integers and school method to multiply the runtime is $O(n^2)$

Pf (i) induction on i. ...

(ii) Prove by induction that (I) $\gcd(r_{i+1}, r_i) = \gcd(r_i, r_{i-1})$ and prove that (II) $\gcd(r_{\ell+1}, r_\ell) = \gcd(0, r_\ell) = r_\ell$.

Interludium

Given $a, b \in \mathbb{Z}$ we define their greatest common divisor to be ~~the~~ a number g with

(a) $g \mid a \wedge g \mid b$

(b) $\forall d: d \mid a \wedge d \mid b \Rightarrow d \mid g$

or $d \leq g$

"Notation": $g =: \gcd(a,b)$.

(I) Note that $r_{i+1} = -q_i r_i + r_{i-1}$.

Now let $g = \gcd(r_i, r_{i-1})$. Then $\underbrace{g \mid r_i}_{g \cdot u_i = r_i}$, $g \mid r_{i-1}$. $g \cdot u_{i-1} = r_{i-1}$

So $r_{i+1} = (-q_i u_i + u_{i-1}) \cdot g$,

i.e. $g \mid r_{i+1}$. So by (b) $g \mid \gcd(r_{i+1}, r_i)$.

Similarly, you get $\gcd(r_{i+1}, r_i) \mid g$. So they are (essentially) equal. □

(II) trivial

Thus we have $r_\ell = \gcd(a,b)$ by induction.

(iii) $\ell < \infty$.

Notice that

$$0 < r_\ell < r_{\ell-1} < r_{\ell-2} \dots < |r_1| = |b|$$

so $\ell \leq |b| < \infty$.

Actually, one can prove that

Ex

$$r_{i+1} \leq \frac{1}{2} r_{i-1} \quad \text{for } 2 \leq i \leq \ell$$

thus if ℓ even

$$0 < \underset{1 \leq}{r_\ell} < \frac{1}{2} r_{\ell-2} < \frac{1}{4} r_{\ell-4} < \dots < \frac{1}{2^{\frac{\ell}{2}-1}} |r_2|$$

thus $2^{\frac{\ell}{2}-1} \leq |r_2| \leq |b|$

thus $\ell/2 \leq \log_2 |b| \leq n$.

so $\ell \in O(n)$.

$\square$

Starter exercise

TriCo 28
17.10.08

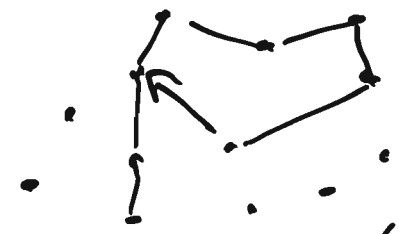
Compute in $\mathbb{Z}_{13}$ all powers of

(i) 2

(ii) 5

(iii) 8

(iv)* 3



Observation 0: We must cycle!

x^i	0	1	2	3	4	5	6	7	8	9	10	11	12
2	1	2	4	8 (−5)	3	6	−1	−2	−4	−8 (−5)	−3	−6	1
5	1	5	−1	−5	1	.	.	.	.				1
8	1	8	−1	−8	1	.	.	.	.	.			1
3	1	3	−4	1	.	.	.	.	.	.	.		1
4	1	4	3	−1	−4	−3	1	.	.	.	.	.	1

Observation 1: We always get back to the starting point 1.

−1	1	−1	1	.	.	.	.	.	.	.	.	.	1
1	1	1	.	.	.	.	.	.	.	.	.	.	1

Observation 2: The length of every cycle divides 12.

Observation 2': For every $x \in \mathbb{Z}_{13} \setminus \{0\}$ we have $x^{12} = 1$.

Another example: in $\mathbb{Z}_6$ what are the powers of 2?

$1 \quad 2 \xrightarrow{\cdot 2} -2 \quad +2 \boxed{\text{not } 1} \;\|\; 1 \quad -1 \quad 1$

in $\mathbb{Z}_8$:

1	3	1				
1	2	4	0	0	...	$\boxed{\text{not } 1}$

in $\mathbb{Z}_{14}$:

	x						$\gcd(x, 14)$
1	2	4	−6	$\boxed{2}$	not 1		2
1	3	−5	−1	−3	5	1	1
1	4	...	not 1				2
1	5	...				1	1
1	6	...	not 1				2
1	7	$\boxed{7}$	not 1				7

Observation 3:

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

Then for $x \in \mathbb{Z}_N$ with $\gcd(x,N) = 1$

we observe $\quad x^{\varphi(N)} = 1 \quad$ in $\mathbb{Z}_N$

<u>for all our examples</u>

Note that only work with multiplication and only those elements that ... are invertible.
because of the

<u>Corollary</u>

$x \in \mathbb{Z}_N$ is invertible

$\Leftrightarrow$ EEA ~~gives~~ reaches 1

ie. $\gcd(N, x) = 1$.

<u>Def</u>

$$\mathbb{Z}_N^\times := \{ x \in \mathbb{Z}_N \mid x \text{ invertible (wrt. multiplication)} \}$$

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

... $\mathbb{Z}_N$: PANICT
PANIC.
D OT 1.

?

$\mathbb{Z}_N^\times$ P.ANIC

So $\mathbb{Z}_N^\times$ should be a commutative group.

<u>Observation</u> with $N=2$ $\mathbb{Z}_N^\times = \{1\}$.
And $1+1=0 \notin \mathbb{Z}_N^\times$ so we cannot restrict addition to this set.

ie: The sum of invertible elements needs not be invertible.

Thm $(\mathbb{Z}_N^\times, \cdot)$ is a commutative group.

Pf **P.** We have to show that product of two invertible elements is again invertible.

Given $x, y \in \mathbb{Z}_N^\times$. Say $ax = 1$, $by = 1$.

Then $$(ba)(xy) = b\underbrace{(ax)}_{=1}y = b\underbrace{y}_{=1} = 1$$

ie xy has the inverse ba, so it is invertible. ✓

A. trivial

N. 1 is invertible: $1 \cdot 1 = 1$

I. Given $x \in \mathbb{Z}_N^\times$. Say $a \cdot x = 1 = x \cdot a$

Then a is also invertible!

(ie. $xa = 1 = ax$)

Thus the inverse a of x does exist in $\mathbb{Z}_N^\times$.

C. trivial.

$\square$

Fact $(\mathbb{Z}_N, +)$ is also a commutative group. (Forget multiplication.)

Further example: the set of invertible matrices is a (usually non-commutative) group.

For now let

G be any finite group.
(written multiplicatively).

<u>Thm</u> (Lagrange 17xx)

For any $x \in G$ we have $x^{\#G} = 1$ in G.

<u>Pf</u> in case G is additionally commutative.

Let $a_1, a_2, \ldots, a_{\#G}$

be a list of all elements of G
(without repetitions or omissions).

Multiply each list element by x:

$$xa_1, \; xa_2, \; \ldots, \; x\,a_{\#G}.$$

Claim: this is again a list of all group elements without repetitions and omissions.

<u>Pf</u> (i) $xa_i \in G$.

(ii) no repetitions: assuming $xa_i = xa_j$
we get by multiplying with x^{-1} (We are in a group!)

$$a_i = a_j$$

so $i = j$.

(iii) no omissions: Take any element from G, say a_i.
Want to that $xa_j = a_i$ for some j.
Obviously, $x^{-1}a_i$ is a group element, so it's on the first list

thus $x^{-1}a_i = a_j$ for some j.

But then $a_i = x a_j$

ie. a_i is on the second list.

(iv) both lists are finite. ∎

Thus both lists are equal up to order.
So multiplying should give the same result since by commutativity order does not matter.

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{\#G} = xa_1 \cdot xa_2 \cdot \ldots \cdot x a_{\#G}$$

so

$$\underbrace{a_1 a_2 \ldots a_{\#G}} = x^{\#G} \cdot \underbrace{a_1 a_2 \ldots a_{\#G}}_{\in G},$$

divide by b then:

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

<u>Corollary</u> (Euler's theorem) (7??)
For $x \in \mathbb{Z}_N^\times$ we have $x^{\varphi(N)} = 1$ in $\mathbb{Z}_N^\times$,
where $\varphi(N) = \# \mathbb{Z}_N^\times$.

<u>Pf</u> $\mathbb{Z}_N^\times$ is a finite group, so by Lagrange we are done. $\square$

Corollary (Fermat's little theorem 16??)

Assume p is prime,
and $x \in \mathbb{Z}_p^\times$, i.e. $p \nmid x$.
Then
$$x^{p-1} = 1 \quad \text{in } \mathbb{Z}_p^\times.$$

Proof By Euler's theorem it suffices to show that $\# \mathbb{Z}_p^\times = p-1$.
But that's clear from
$$\mathbb{Z}_p^\times = \{ x \in \mathbb{Z}_p \mid \underbrace{\gcd(x,p) = 1}_{p \nmid x} \}$$
$$\overset{\shortparallel}{\{ \cancel{0}, 1, 2, \dots p-1 \}}. \qquad \square$$

Theorem RSA is ~~(almost)~~ correct for almost all $x \in \mathbb{Z}_N$.

Proof Given $x \in \mathbb{Z}_N^\times$, $N = p \cdot q$, $L = (p-1)\cdot(q-1)$.
We have to prove that $z = y^d$, $y = x^e$,
$$z = x.$$
Now
$$z = (x^e)^d = x^{e \cdot d} = x^{1 + k \cdot L} = x \cdot (x^L)^k$$
By Euler (or Lagrange) we know that $x^{\# \mathbb{Z}_N^\times} = 1$.
So it is enough to show that $L = \# \mathbb{Z}_N^\times$!

Because then
$$z = x \cdot (x^L)^k = x \cdot 1^k = x,$$
so we are done.

By the following Lemma we fill the gap. $\square$

<u>Lemma</u> Let $N = p \cdot q$ be a product of two <u>different</u> primes p, q.

Then
$$\# \mathbb{Z}_N^\times = (p-1) \cdot (q-1).$$

<u>Proof</u> By definition (or a small fact)
$$\mathbb{Z}_N^\times = \{ x \in \mathbb{Z}_N \mid \gcd(x, N) = 1 \},$$
or
$$\mathbb{Z}_N \setminus \mathbb{Z}_N^\times = \{ x \in \mathbb{Z}_N \mid \gcd(x, N) \neq 1 \}.$$
We know that $\gcd(x, N) \in \{1, p, q, p \cdot q\}$.

Thus
$$\mathbb{Z}_N \setminus \mathbb{Z}_N^\times = \{ x \in \underset{\{0,1,\dots,pq-1\}}{\underset{\shortparallel}{\mathbb{Z}_N}} \mid p \mid x \vee q \mid x \}.$$

so
$$\#(\mathbb{Z}_N \setminus \mathbb{Z}_N^\times) = q + p - 1.$$

and
$$\# \mathbb{Z}_N^\times = p \cdot q - q - p + 1$$
$$= (p-1)(q-1). \qquad \square$$

Actually: $\mathbb{Z}_N^\times$ is almost all of $\mathbb{Z}_N$ in the RSA case:

$$\text{prob}\left(x \notin \mathbb{Z}_N^\times \mid x \in_R \mathbb{Z}_N \right)$$

$$= \frac{\#(\mathbb{Z}_N \setminus \mathbb{Z}_N^\times)}{\# \mathbb{Z}_N}$$

$$= \frac{p+q-1}{pq}$$

$$\approx \frac{2 \cdot 2^{n/2}}{2^n} = 2^{-n/2+1} \doteq 2^{-511}.$$

In practice, $n = 1024$ (or larger).

This is as good as zero, and so in practice we have proved RSA correct.

In fact, RSA is also correct for the remaining cases, yet our proof doesn't show it.

Ex: Proof that RSA is correct.

Solution 1:

RSA is correct for $x \in \mathbb{Z}_N^\times$.

& $\text{prob}(x \notin \mathbb{Z}_N^\times) \approx 0$

Solution 2:

RSA is correct.

Let's have a look at prime generation.

- p is prime iff its only divisors are $\pm 1, \pm p$.

~~(ii) For any $x \in \mathbb{Z}$~~

- If p is prime then
$$\forall x \in \mathbb{Z}_p^\times : \quad x^{p-1} = 1.$$
- If p is prime then $\mathbb{Z}_p$ is a field
(ie. $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$).

in particular:
$$\#\{x \in \mathbb{Z}_p \mid x^2 = 1\} \leq 2.$$

This leads to the (strong) Fermat test:

<u>Fermat test</u>

Input: a number N.
Output: YES, it may be prime.
NO, it <u>is</u> not a prime.

1. Pick a random $x \in_R \mathbb{Z}_N^\times$.
2. Compute $y := x^{N-1}$ in $\mathbb{Z}_N$. $O(n^3)$
3. Return $\begin{cases} \text{YES} & \text{if } y = 1, \\ \text{NO} & \text{if } y \neq 1. \end{cases}$

This gives a good answer but fails CARMICHAEL numbers: 561 ... but otherwise

$$\text{prob}(\text{Fermat test answers YES} \mid N \text{ is not prime}) \leq \tfrac{1}{2}.$$

Strong Fermat test (Miller 1976, Rabin 1980)

input: a number N

Output: YES, it may be prime.
NO, it is not a prime.

1. Pick a random $x \in_R \mathbb{Z}_N^\times$.
2. Write $N-1 = t \cdot 2^s$ with t odd, $s \geq 0$.
   (i.e. $N-1$ finishes with s zero bits in the binary representation).
3. Compute $y_0 := x^t$,
   $y_1 := y_0^2$, $O(n^3)$
   $\vdots$
   $y_s := (y_{s-1})^2$.

   $y_i^2 = 1$ but $y_i \neq 1, -1$. So $\#\{\ldots x^2 = 1\} \geq 2$. $\Rightarrow$ N prime

4. If $y_s \neq 1$ then Return (NO)
5. If $y_0 = 1$ then Return (YES)
6. If $y_i \neq \pm 1$, $y_{i+1} = 1$ then RETURN(NO)
7. Otherwise Return (YES)

Theorem

$$\text{prob}\left(\text{Strong Fermat test says YES} \;\middle|\; N \text{ is not prime}\right) \leq \frac{1}{4}.$$

$\square$

So

$$\text{prob}\left(\text{Strong Fermat test says YES 17 times} \;\middle|\; N \text{ is not prime}\right) \leq \frac{1}{4^{17}}.$$

So to find a prime with $\frac{n}{2}$ bits do this:

Repeat
Pick a random number N with $\frac{n}{2}$ bits.
Run the Strong Fermat test on it a few times
Until the answer is YES (it may be prime).

<u>Fact</u> run time (✓) $= O(n)$ iterations.

because of the famous Prime Number Theorem (1896)

With $\pi(B) := \#\{n \le B \mid n \text{ is prime}\}$

we have
$$\frac{\pi(B)}{B} \approx \frac{1}{\ln B}.$$

In our case $B = 2^{n/2}$ so

$$\frac{\pi(2^{n/2})}{2^{n/2}} \approx \frac{2}{n \ln 2} = \frac{2/\ln 2}{n}$$

Thus the expected number of trials to find a prime is $\dfrac{n}{2/\ln 2}$.

Summary

- RSA is correct (in practice).

- RSA is efficient

generate keys
- generate a prime = n guesses and prime tests so $O(n^4)$
- multiply $O(n^2)$
- EEA $O(n^2)$

encrypt / decrypt
- exponentiation $O(n^3)$

- RSA ... Is it secure?

What does it <u>mean</u> that RSA is secure?

- No attacker should be able to break RSA...

What does it mean to break RSA?

FACTORING.

(1) $\boxed{\text{Given } (N, e, y) \text{ find } p, q.}$

find L.

(2) [Actually, $(x-p)(x-q) = x^2 - (N-L+1)x + N$, ...]

find d.

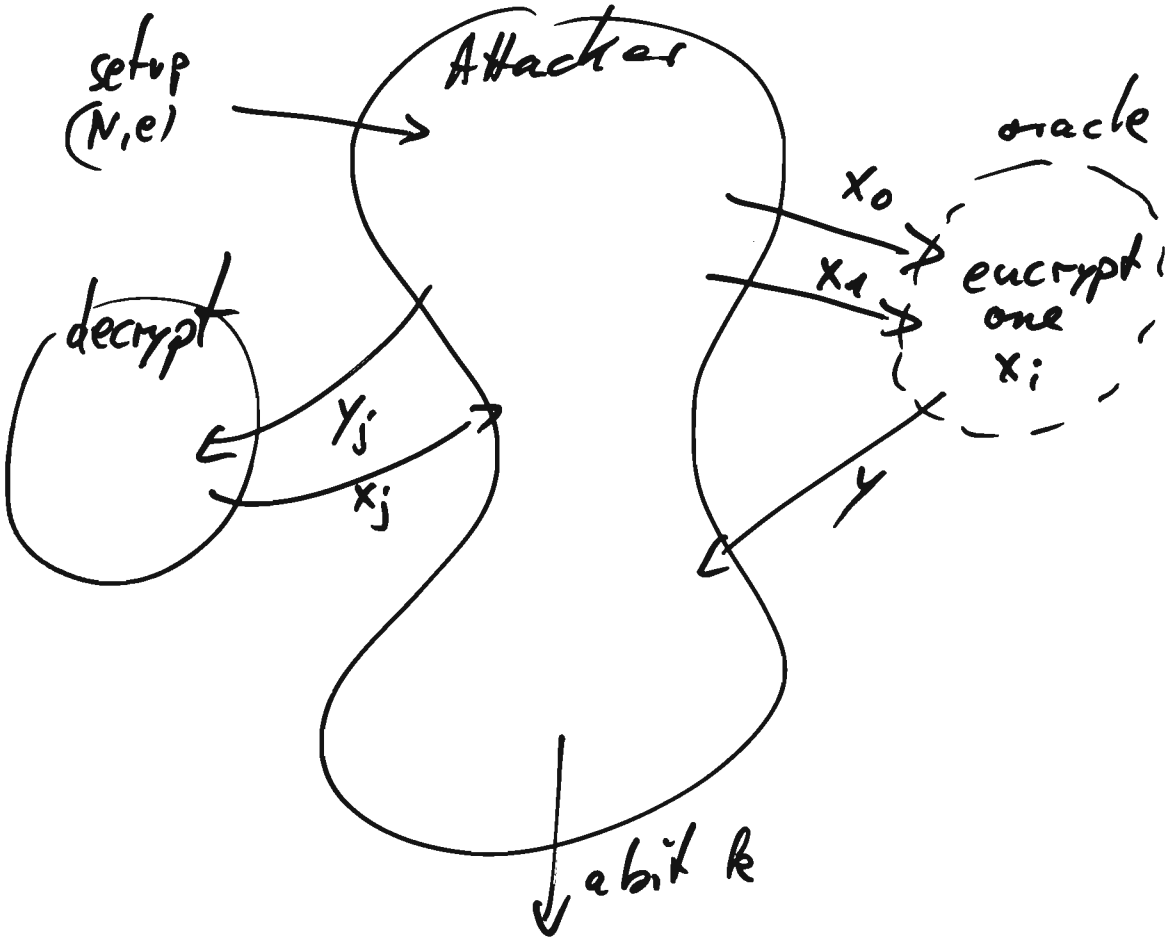
(3) [Then you can decrypt... But also $L \mid (ed-1)$.
This is not enough to find L. But if you can another d' corresponding to another e' then $L \mid (e'd'-1)$,
so $L \mid \underbrace{\gcd(ed-1, e'd'-1)}$, usually
this is at most $\leq 10 \cdot L$.

find x

Well, is that the story?

Security model

Strongest version:



Goal: $i = k$ &

without ever asking y to the decrypt-oracle.

Attack succeeds if

$$\text{prob}(\, i = k \text{ without asking } y) \gg \frac{1}{2}.$$

RSA is <u>not</u> secure in this sense.

Yet, RSA is useful and probably secure in a weaker sense. provided that FACTORING is difficult.

Leftover: Chinese Remainder Theorem.

Teacher is on a walk with his class.
Wants the pupils to arrange nicely.
Say in rows of two: 1 pupil remaining.
in rows of three: 1 remaining
in rows of five: 0 !

Trying multiples of 5 shows:
it could be 25 pupils.
But also 55 fits...

Let's start with only two conditions:

$$x \equiv_m a \qquad (m \mid (x-a))$$

$$x \equiv_n b \qquad (n \mid (x-b))$$

ie.

$$x = a + k \cdot m \quad \text{for some } k$$
$$x = b + \ell \cdot n \quad \text{for some } \ell$$

So in particular we have

$$a + km = b + \ell n$$

or

$$(k) \cdot m + (-\ell) \cdot n = b - a$$

We could directly attack this using the EEA. It gives g, s, t so that

$$s m + t n = g$$

If now $g \mid b-a$ then

$$\left(\frac{b-a}{g} \cdot s\right) m + \left(\frac{b-a}{g} \cdot t\right) n = b - a$$

To give it more shape stand back:

Assume $a = 0$, $b = 0$.
Then we get to the problem

$$s \cdot m + t n = +1.$$

This we get from EEA provided m, n have no common factor. Now read that equation modulo m and n:

mod m

$$\boxed{t n} \equiv_m 1 \qquad \boxed{s m} \equiv_m 0$$

$$\boxed{s n} \equiv_n 0 \qquad \boxed{s m} \equiv_n 1$$

Thus $x_0 = a \cdot tn + b \cdot sm$ solves the original problem.

Thm Given m, n coprime, ie. $\gcd(m,n)=1$.
Then for every a, b we can find x_0 such that

$$x_0 \equiv_m a$$

and

$$x_0 \equiv_n b$$

and actually every solution x of this is equal to x_0 modulo $m \cdot n$.

Proof $EEA(m,n) \to sm + tn = 1$.
Then $x_0 = a \cdot tn + b \cdot sm$ does it.

Given any x with

$$x - x_0 \equiv_m 0$$

$$x - x_0 \equiv_n 0$$

then $m \mid x - x_0$ and $n \mid x - x_0$ and

since m, n are coprime so $m \cdot n \mid x - x_0$

ie. $x \equiv_{m \cdot n} x_0$.

~~Now using this for $x = x_0$~~ $\square$

Corollary Given m, n coprime. 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 an isomorphism.

<u>Example</u> $6 = m=2,\ n=3$

$$\mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$\begin{aligned}
0 &\longmapsto (0,\ 0)\\
1 &\longmapsto (1,\ 1)\\
2 &\longmapsto (0,\ 2)\\
3 &\longmapsto (1,\ 0)\\
4 &\longmapsto (0,\ 1)\\
5 &\longmapsto (1,\ 2)
\end{aligned}$$

$\mathbb{Z}_2 \backslash \mathbb{Z}_3$	0	1	2
0	0	4	2
1	3	1	5

so $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

<u>Another ex</u>

$\mathbb{Z}_2 \backslash \mathbb{Z}_2$	0	1
0	0,2	$\boxed{?}$
1	$\boxed{?}$	1,3

so $\mathbb{Z}_4 \neq \mathbb{Z}_2 \times \mathbb{Z}_2$.

This leads to:

<u>Thm</u> Given m, n coprime. Then

$$\mathbb{Z}_{m \cdot n}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$$

so

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

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

BriCo (5a)
17.10.08

Example run of RSA

(1) Find two primes p, q

$p = 11$

$q = 13$

(2) $N = 11 \cdot 13 = 143.$

(3) $L = 10 \cdot 12 = 120.$

(4) Find e, d with $ed \equiv_L 1.$

$e = 7 \quad d = ?$

	r	q	s	t
$L =$	120		1	0
$e =$	7	17	0	1
	1	7	1	-17
	0		-7	120

$\boxed{\text{Xcheck ok}}$

$1 = 1 \cdot 120 + (-17) \cdot 7$

thus $d = -17 = 103.$

(5) Return public key $(143, 7)$

private key $(143, 103)$

$$\begin{array}{r} 729 \\ -143 \cdot 5 \\ \hline 14 \end{array}$$

<u>Encrypt</u> $x = 3$: $3 \xrightarrow{\cdot^2} 9 \xrightarrow{\cdot 3} 27 \xrightarrow{\cdot^2} 14 \xrightarrow{\cdot 3} 42$

$\boxed{y = x^7 \text{ in } \mathbb{Z}_{143}}$ $\quad y = 42.$

<u>Decrypt</u> $y = 42 \longrightarrow z = y^{103}$ in $\mathbb{Z}_{143}$ you should obtain $z = 3.$