Brico (1) 15.10.07

→ list of names

- SEND AN EMAIL TO NUESKEN@BIT.UNI-BONN.DE

→ Set up an account for b-it computers!

How to?

→ Encrypt: she encrypts.
he decrypts.

– need 'shared' key

But ~~when~~ if Monica sends the key then Michael (Eve, ...) gets it.

Need 'secure channel' for that or a completely different idea.

Traditional/classical:

Symmetric

Cesar cipher

~~ZABC~~

A B C D E F .... W X Y Z

D E F ---- Z A B C

3rd successor

BRIDGE ⟶ EULGJH

⟵

3rd predecessor

KEY

26 possible ones (though one is trivial)

Encrypt: simple

Decrypt: simple

Break: too simple. Brute force does it.

Better?

- Replace letters by numbers.
- Use longer key.

A = 0
B = 1
C = 2
!
Z = 25

BRIDGING COURSE
\+ SECRET SECRET SECRET

TVK---

Encrypt: Simple
Decrypt: Simple
Break: Frequency analysis + a bit

With a six letter key we now have

26^6 [26 to the 6th].

Better?

- Use a permutation of the letters
  (→ long key!
  # keys = 26! ~ 10^{26} ~ 2^{85}

encrypt(+ B C D (E) F G ...) decrypt.
         U X A C Y W O Q ...

Brute force is no solution.
Too many keys.

But frequency analysis breaks it!

Encrypt: simple.
Decrypt: simple
Break: easy.

Better?

- Use the 'word' scheme
  with a key (i) as long as message
  (ii) completely random.

→ One Time Pad
key = bit sequence (random)
plain msg = bit sequence
cipher text = bitwise XOR of key and msg.

Encrypt: Simple
Decrypt: simple
Break: Provably, absolutely impossible!

But too long key.

Use key twice?

$C_1 = M_1 \oplus K$

$C_2 = M_2 \oplus K$

Eve has C_1, C_2:

$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$

$= (M_1 \oplus M_2) \oplus \underbrace{(K \oplus K)}_{=0}$

$= M_1 \oplus M_2$

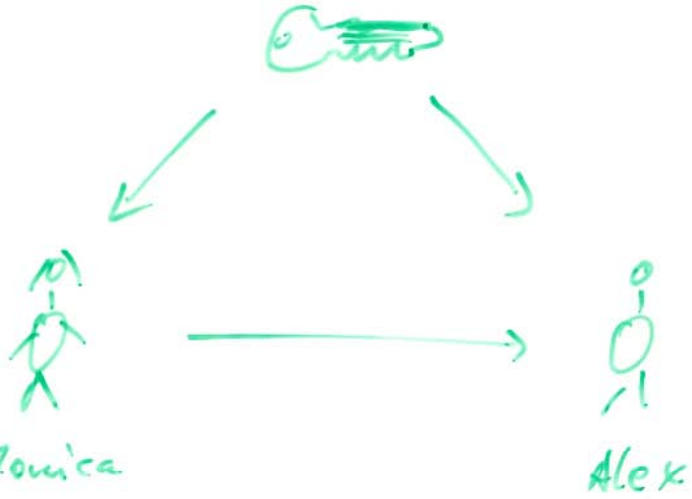
Broken.

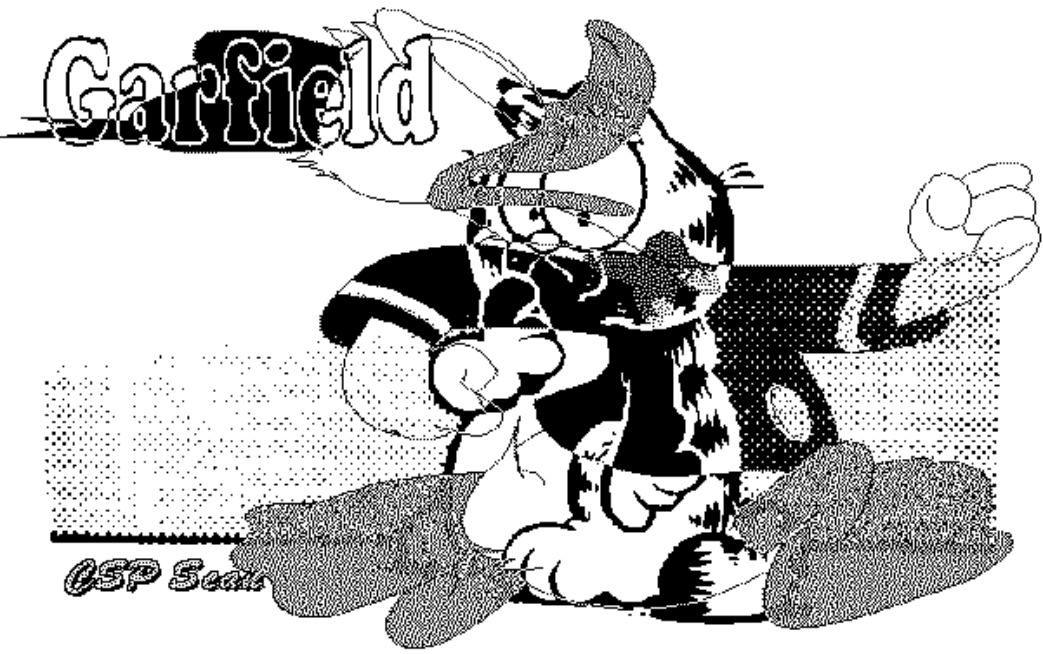
Two Time Pad

→ (3)DES works: 2^{112} keys
in use since about 1977

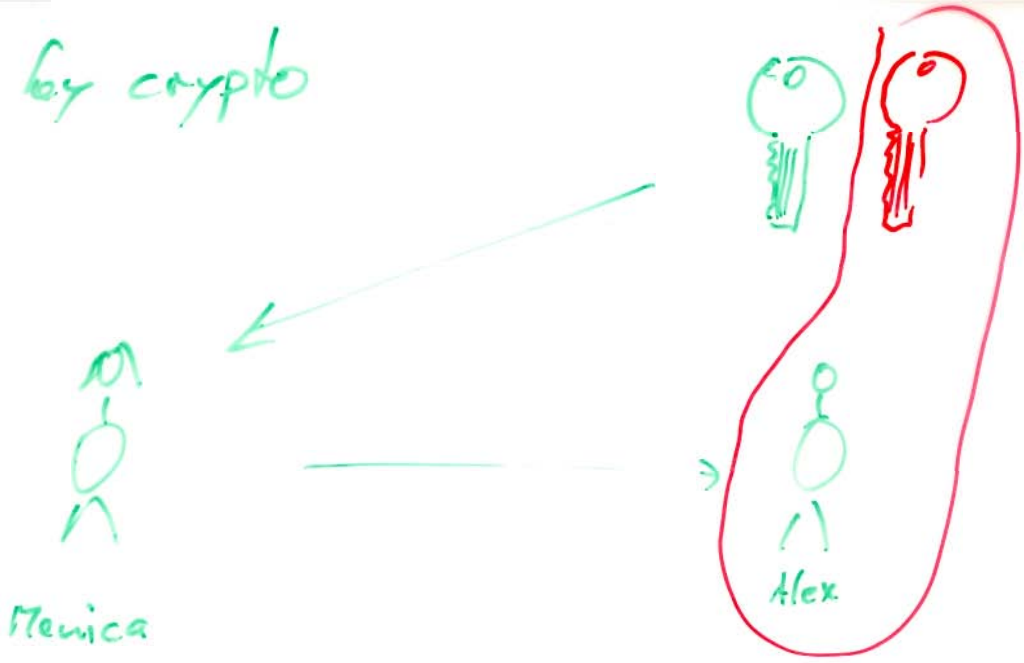
AES works: 2^{128} keys
three year competion
~ 2002

Still situation




Garfield
CSP Scan

Public key crypto



RSA (Rivest, Shamir, Adleman 1978)

Setup (Alex)

- Generate two (different) random primes p, q
  say each is about 512 bits long
- $N = p \cdot q$ modulus
- $L = (p-1)(q-1)$ repetition length
- Throw away p, q num.
- Generate $e \in \mathbb{Z}_L^* = (\{0, 1, 2, \dots, L-1\}, +, \cdot)$ (operations modulo L)
- Compute $d \in \mathbb{Z}_L$ such that

$$e \cdot d = 1$$

[Choose $e \in \mathbb{Z}_L$, try to find d, repeat until possible.]

- Public key $= (N, e)$ [for encrypting]
- Private key $= (N, d)$ [for decrypting]
- Throw anything else.

Send public key to Monica & the world.

Encrypt (Monica) She knows public key (N, e)

Encode the message as $x \in \mathbb{Z}_N$.

(Note that N is an (about 1024) bit-number.)

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

Decrypt (Alex) He knows private key (N, d).

Decrypt: $z = y^d$ in $\mathbb{Z}_N$

It turns out that $z = x$. CORRECTNESS

And all operations can be done fast. EFFICIENCY

It should be "unbreakable". SECURITY.

Fast: • less than $O(n^2)$ $\quad n$ # input (in bits)

• less than a minute.

Slow: $O(2^n)$

Exam: after week 4, march.
compolsary for those
for who the course is.

Ring of integers modulo N

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

optionally: 0, 1, −, division? inverse?

Implementation: integers, ≥ 0, $< N$

for $a, b \in \mathbb{Z}_N$

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

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

Sideremark on notation: $\hat{a}$ rem $N \in \mathbb{Z}$, ← integers

$\hat{a} \bmod N \in \mathbb{Z}_N$.

for $\hat{a} \in \mathbb{Z}$, $N \in$ ~~$\mathbb{Z}$~~ $N_{\geq 2}$

(or $\hat{a} \in \mathbb{Z}_N$)

Excursion

17 rem 11 = 6 because $17 = 1 \cdot 11 + 6$,
$0 \leq 6 < 11$.

1 $23 \bmod 14 = 9$

$(23 \bmod 14) + (5 \bmod 7) =$ FAIL

$(23 \bmod 14) +_{\mathbb{Z}_{14}} (5 \bmod 14) = 0 \bmod 14 = 0 \quad \in \mathbb{Z}_{14}$

$(23 \text{ rem } 14) +_{\mathbb{Z}} (5 \text{ rem } 14) = 14 \quad \in \mathbb{Z}$

The ring of integers modulo N

Brilo
15.10.07
(8)

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

~~0:~~ 0

$P_{+,\cdot}$ properly defined, i.e. $+$ is as claimed and in particular $a+b \in \mathbb{Z}_N$ for all $a,b \in \mathbb{Z}_N$.

$A_{+,\cdot}$ associative $(a+b)+c = a+(b+c)$

$N_{+,\cdot}$ neutral element: $\exists\, 0 \in \mathbb{Z}_N : \forall a \in \mathbb{Z}_N : a+0 = a = 0+a$

$\exists\, 1 \in \mathbb{Z}_N : \forall a \in \mathbb{Z}_N : a \cdot 1 = a = 1 \cdot a$

$I_{+,}$ ~~$\cdot$~~ inverses exist: $\forall a \in \mathbb{Z}_N\ \exists b \in \mathbb{Z}_N : a+b = 0 = b+a$

$C_{+,\cdot}$ commutative: $\forall a,b \in \mathbb{Z}_N : a+b = b+a$

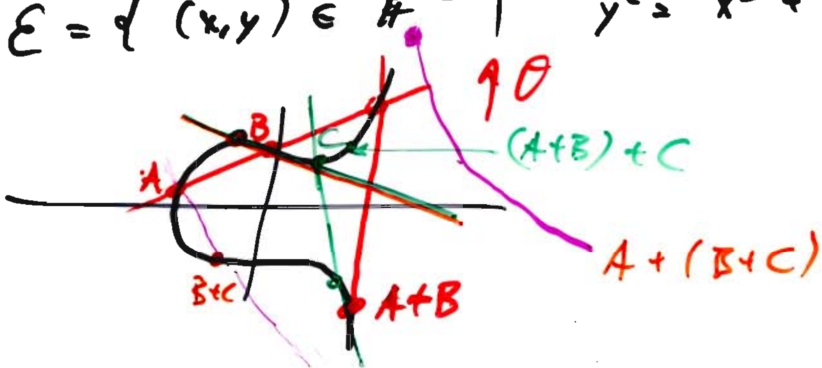
D distributive: $a\cdot(b+c) = ab+ac$

commutative Ring: PANIC+, PANC·, D, O

$0 \neq 0+1.$

Set with a commutative addition law where A_+ is difficult to see (say $\mathbb{F} = \mathbb{R}, \ldots$)

$\mathcal{E} = \{ (x,y) \in \mathbb{F}^2 \mid y^2 = x^3 + ax + b \} \cup \{\mathcal{O}\}$ with a,b given $a=b=1$.



... elliptic curve

So simple:

time $(a +_{\mathbb{Z}_N} b) \in O(n)$

where N is an n-bit number.

time $(a \cdot_{\mathbb{Z}_N} b) \in$?

school method multiplication

$+ d$

} price : $2n^2$

$O(n^2)$

Karatsuba multiplication (half size)

$(a_1 g + a_0) \cdot (b_1 g + b_0)$

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

$(a_1 + a_0) \cdot (b_1 + b_0) - a_1 b_1 - a_0 b_0$

→ 3 op's of half size

↳ $O(n^{\log_2 3}) \approx O(n^{1.58})$

Schönhage-Strassen multiplication ('71)

(in BONN)

$O(n \log n \log\log n)$

Fürer (2007)

$O(n \log n \, 2^{\log^* n})$

Division with remainder: price is the same!

So time $(a \cdot_{\mathbb{Z}_N} b) \in \mathcal{O}(n^2)$

What about division in the ring $\mathbb{Z}_N$?

Recall that for integers we have division with remainder: Given $a, b \in \mathbb{Z}$, $b \neq 0$ there exist $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r, \quad 0 \leq r < |b|$$

Cost: $\mathcal{O}(n^2)$ [or faster with fast methods...]

Division? or say, modularly: inversion in $\mathbb{Z}_N$?

We are given $e \in \mathbb{Z}_N$
and we look for $d \in \mathbb{Z}_N$
such that $e \cdot d = 1$ in $\mathbb{Z}_N$.

(L instead of N)

Translate this to integers:

We are given $e \in \mathbb{Z}$, ~~$(0 \leq e < N,)$~~
and we look for $d \in \mathbb{Z}$, ~~$(0 \leq d < N,)$~~
such that $d \cdot e + k \cdot N = 1$

for some (also unknown) $k \in \mathbb{Z}$. ~~$(0 \leq k < N)$~~

So our task is this:

> Given $a, b \in \mathbb{Z}$ and
> look for $s, t \in \mathbb{Z}$
> such that $s \cdot a + t \cdot b = 1$ ..

Ex $a = 15$, $b = 34$. Aim: $s \cdot a + t \cdot b$ very small

	r	q	s	t	Comment $s \cdot a + t \cdot b = r$
	$a = 15$		1	0	$1 \cdot a + 0 \cdot b = 15$ | $\cdot(-2)$
	$b = 34$	0	0	1	$0 \cdot a + 1 \cdot b = 34$ | $\cdot 1$
$L_{34} \to$	15	2	1	0	$1 \cdot a + 0 \cdot b = 15$
$L_{15} \to 0$	4	3	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot 0 = 1$	$-2 \cdot a + 1 \cdot b = 34 - 2 \cdot 15 = 4$
$L_{34} - 2 \cdot L_{15}$	3	1	7	-3	$7 \cdot a + (-3) \cdot b = 3$
	1	3	-9	4	$-9 \cdot a + 9 \cdot b = 1$
	0		34	-15	$34 \cdot a + (-15) \cdot b = 0$

(15 ↑, 34 ↑)

Euclidean Algorithm

Extended Euclidean Algorithm

How to find q?

(i) It doesn't make things wrong if q is not optimal.

(ii) Best q is the one you from division with remainder $34 = 2 \cdot 15 + 4$

where $0 \leq 4 < 15$

EEA Ex. 2 $a=42, b=16$

BriCo 16.10.07 (1)

i		r	q	s	t
0	q:	42	–	-1	0
1	s:	16	2	0	1
2		10	1	1	-2
3		6	1	-1	3
:		4	1	2	-5
		2	2	-3	8
Output:		0	–	8	-21

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

$42 = 2 \cdot 16 + 10$

Look at the check:

$$0 = \underbrace{8}_{16/2} \cdot 42 + (-21) \cdot \underbrace{16}_{-42/2}$$

Multiply the line by its q and subtract from the line above it to obtain a new line. Do that until you reach 0 in the r-column.

Output: $2 = -3 \cdot 42 + 8 \cdot 16$

Claim $\forall i \in \mathbb{N}: \gcd(r_i, r_{i+1}) = \gcd(a,b)$ (*)

Pf It is sufficient to proof $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i)$

Note that $a = r_0$, $b = r_1$ and by induction this follows.

$\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i) = \gcd(r_{i-2}, r_{i-1}) = \dots = \gcd(r_0, r_1) = \gcd(a,b)$

Now, $r_{i-1} = q_i \cdot r_i + r_{i+1}$, $q_i, r_{i+1} \in \mathbb{Z}$

r_{i-1}, r_i

Suppose that c divides r_{i-1} and r_i.

Thus $r_{i+1} = \left(\underbrace{\frac{r_{i-1}}{c}}_{\in \mathbb{Z}} - q_i \cdot \underbrace{\frac{r_i}{c}}_{\in \mathbb{Z}} \right) \cdot c$

$\in \mathbb{Z}$

i.e. c divides r_{i+1}, noted as: $c \mid r_{i+1}$.

So c divides r_i and r_{i+1}.

In total: any common divisor of r_{i-1} and r_i is also a common divisor of r_i and r_{i+1}.

In particular, $c = \gcd(r_{i-1}, r_i)$

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

$(\leq)$

Now, suppose that c divides r_i and r_{i+1}.

Thus $r_{i-1} = \left(q_i \cdot \underbrace{\frac{r_i}{c}}_{\in \mathbb{Z}} + \underbrace{\frac{r_{i+1}}{c}}_{\in \mathbb{Z}} \right) \cdot c$

$\in \mathbb{Z}$

so c divides r_{i-1} and r_i. $\in \mathbb{Z}$

Thus $\gcd(r_i, r_{i+1}) \mid \gcd(r_{i-1}, r_i)$.

$(\leq)$

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

□

Observe: $\gcd(a, 0) = a$.

Theorem

The EEA outputs the greatest common divisor g of the input elements a, b and a representation

$$g = s \cdot a + t \cdot b.$$

in at most $\mathcal{O}(\log_2(\min(a,b)))$ rows.

$g = r_e$

$= \mathcal{O}(n)$

Pf Termination: $|r_{i+1}| < |r_i|$!

Thus $e \leq \min(a,b) + 1$.

Fast termination: $|r_{i+1}| \leq \frac{1}{2} |r_{i-1}|$. (Ex)

for $i \geq 2$

Correctness: see above.

□

Ex . $a = 77, b = 20$

. $a = 102, b = 51$ // more interesting: $a = 99, b = 51$

. Compute the inverse of 10 modulo 17.

Corollary The runtime of EEA is in

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

Pf ✓

Actually, it is even in $\mathcal{O}(n^2)$.

↑ Fast multiplication only gives $\mathcal{O}(n^2 \log n \log\log n)$. + Sophisticated divide & conquer → $\mathcal{O}(n(\log n)^3 \lg\lg n)$

Ex Inverse of 10 in $\mathbb{Z}_{17}$:

BiCo 16.10.07 (4)

We look for d such that $d \cdot 10 = 1$ in $\mathbb{Z}_{17}$.

ie: $d, 10, 1 \in \mathbb{Z}_{17}$

$\cdot = \cdot_{\mathbb{Z}_{17}}$

$(\,)^{-1}$ is in $\mathbb{Z}_{17}$.

Equivalently:
we look for d, k such that

$$d \cdot 10 + k \cdot 17 = 1 \text{ in } \mathbb{Z}.$$

A solution for this we get using EEA:

	r	q	s	t
b	17		0	1
a	10	1	1	0
	7	1	-1	1
	3	2	2	-1
	1	3	-5	3
	(0)		17	-10

Check: $0 = 17 \cdot (-10) + (-10) \cdot 17$

Output: $1, -5, 3$ ie $1 = -5 \cdot 10 + 3 \cdot 17$ in $\mathbb{Z}$.

Thus in $\mathbb{Z}_{17}$:

$1 = (-5) \cdot 10 + 3 \cdot 0$ in $\mathbb{Z}_{17}$.

Answer: $-5 = 12$ in $\mathbb{Z}_{17}$.

Check: $12 \cdot 10 = 1$ in $\mathbb{Z}_{17}$.

$[120 = 7 \cdot 17 + 1.]$

Brilo
16.10.07
(5)

Ex What's the inverse of 6 in $\mathbb{Z}_{10}$?

Start the EEA with $a = 10$, $b = 6$:

10		0	1
6	2	1	0
−2	−3	−2	1
(0)		−5	3

Check: $0 = -5 \cdot 6 + 3 \cdot 10$ ✓

$-\frac{10}{-2}$ $\quad -\frac{6}{-2}$

Output:

$-2 = (-2) \cdot 6 + 1 \cdot 10.$

gcd $\quad s \quad t$

Or:

$2 = 2 \cdot 6 + (-1) \cdot 10.$

Theorem Given a in $\mathbb{Z}_N$, the EEA computes s, t, g such that

$$g = s \cdot a + t \cdot N$$

with $g = \gcd(a, N)$.

Case 1 $g \neq 1$. Then no inverse of a in $\mathbb{Z}_N$ exists!

Case 2 $g = 1$. Then $s \bmod N$ is the inverse of a in $\mathbb{Z}_N$.

Def $\mathbb{Z}_N^\times := \{ a \in \mathbb{Z}_N \mid \exists b \in \mathbb{Z}_N : ab = 1 \in \mathbb{Z}_N \}$.

Zn'Co
16.10.07

Corollary $\mathbb{Z}_N^\times = \{ a \bmod N \mid 0 \le a < N, \gcd(a, N) = 1 \}$ □

Claim: $\mathbb{Z}_N^\times$ is a commutative group wrt. to multiplication (ie. PANIC.)

Pf P.: Suppose $a, a' \in \mathbb{Z}_N^\times$.
To show: $a \cdot a' \in \mathbb{Z}_N^\times$
We have: $ab = 1$, $a'b' = 1$
for some $b, b' \in \mathbb{Z}_N$

Then: $(aa')(bb') = 1$ ✓

A.: ✓ ... $(ab)c = a(bc)$

N.: $1 \in \mathbb{Z}_N^\times$ ✓

C.: ✓ ... $ab = ba$

I.: Suppose $a \in \mathbb{Z}_N^\times$.
Then there is $b \in \mathbb{Z}_N$: $a \cdot b = 1$.
Vice versa: $b \cdot a = 1$ ie. $b \in \mathbb{Z}_N^\times$.
And $ab = 1$, ie. $a^{-1} = b \in \mathbb{Z}_N^\times$ □

Definition $\mathbb{Z}_N^\times$ unit group of $\mathbb{Z}_N$.

BriCo 16.10.07 (7)

Still to do:

- fast exponentiation and repetition length
- RSA is correct...
  - → When is $\mathbb{Z}_N$ more than just a ring
  - → Chinese Remainder Theorem

Fast exponentiation:

2^{54} in $\mathbb{Z}_{101}$.

Trivial algo: $1 \cdot \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdots \cdot 2}_{54 \text{ times}}$: 54 mult!

$\underbrace{2 \cdot 2 \cdot 2 \cdots \cdot 2}_{53 \text{ times}}$: 53 mult!

Better?

exponents in binary

$1, 2, 2^2 = 4, 4^2 = 16, 16^2 = 54, \ldots$

0, 1, 10, 100, 1000

free, 2^4, 2^8

$54^2 = -13, (-13)^2 = 68$

100000, 100000

2^{16}, 2^{32}

$2 \cdot 100 + 56 = 2 \cdot (-1) + 56$

need 5 memory cells here :)

$(-13) \cdot 68 = -9$, $-9 \cdot 16 = -53$, ...

110000, 110100

2^{48}, 2^{52}

$-53 \cdot 4 = -10$

2^{54}, 110110

2916

$16 \cdot 29 = -13$

$-884 = 84 + 8 = 92 = -9$

$-212 = -12 + 200 = -12$

Multiplication (Squaring + 3 mult)

Better?

$1 = 2^0$

$2 = 2^1$

$2^2 = 4 = 2^2$ 10

$8 = 2^3$ 11

$8^2 = 64 = 2^6$ 110

$64^2 = 56 = 2^{12}$ 1100

$56 \cdot 2 = 11 = 2^{13}$ 1101

$11^2 = 20 = 2^{26}$ 11010

$20 \cdot 2 = 40 = 2^{27}$ 11011

$40^2 = -16 = 2^{54}$ 110110

$54 = 110110_2$

5 squarings

3 multiplications

but only 0 additional memory!

Square-and-multiply

(Repeated squaring)

Thm The cost of one exponentiation in $\mathbb{Z}_N$ is $4n^3 \in O(n^3)$.

Observation: We never calculate the integer 2^{54} in the above example!

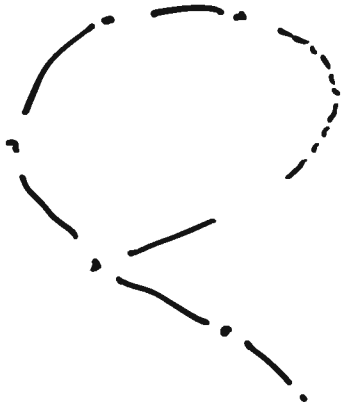
That's essential!

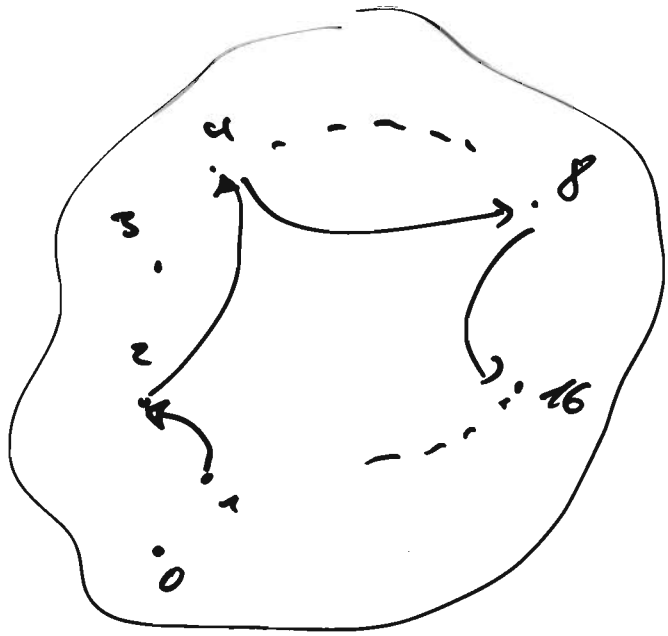
Brilo
16.10.07
(9)

Consider the list:

$$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, \ldots \quad 2^{6314}$$

in $\mathbb{Z}_{101}$.





Since $\#\mathbb{Z}_{101} = 101$

latest 2^{101} must meet a prior number! Actually, there are at most 100 possible outcomes! $2^n \neq 0$.

It turns out that $2^{100} = 1$.

In particular, we have

$$2^{6314} = 2^{14}.$$

$$(2^{100})^{63} \cdot 2^{14}$$

BriCo
16.10.07
(10)

Thm (Lagrange)

Suppose G is a (commutative) group.
Then for any $x \in G$ we have

$$x^{\#G} = 1 \quad \text{in } G.$$

Pf Suppose

$$a_0, a_1, a_2, \ldots, a_{x-1}$$

is a list of all group elements, $x = \#G$.
Multiply all of them by x:

$$xa_0, xa_1, xa_2, \ldots, xa_{x-1}.$$

1. observation: all group elements occur!

⌜ Suppose you look for a_i
Find $x^{-1}a_i$ on the first list: $x^{-1}a_i = a_j$ for some j.

Then $a_i = xa_j$, so a_i is somewhere on the second list! ⌟

2. observation: no duplication in second list.

⌜ Suppose $xa_i = xa_j$ for some $i \neq j$.
Multiply with x^{-1}: $a_i = a_j$. ↯ ⌟

3. observation: both list have x elements.

Any two of the three observations show that the two lists are equal up to order.

Multiply all elements of the first list and compare with the same for second list:

$$a_0 \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} = xa_0 \cdot xa_1 \cdot xa_2 \cdot \ldots \cdot xa_{n-1}$$

↑ Because the lists are equal up to order and the group is commutative.

Divide by the l.h.s.:

$$1 = x^n, \quad n = \#G.$$ □

Apply this for $G = \mathbb{Z}_N^\times$:

Thm (Euler)
For any $N \in \mathbb{N}, N \geq 2$ and $x \in \mathbb{Z}$ with $\gcd(x,N) = 1$ we have

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

where $\varphi(N) := \#\mathbb{Z}_N^\times$.

↖ Euler totient function.

Little Fermat Theorem
For any prime p and $x \in \mathbb{Z}$, $0 < x < p$. ($\gcd(x,p) = 1$)

we have $x^{p-1} = 1$ in $\mathbb{Z}_p^\times$.

Ex $p = 101$, $x \in \mathbb{Z}_{101}$, $x \neq 0$: $x^{100} = 1$ in $\mathbb{Z}_{101}$.

In particular: $2^{100} = 1$ in $\mathbb{Z}_{101}$.

Fact

$\mathbb{Z}_N$ is a field (i.e. all non-zero members are invertible)

iff

N is prime

So for p prime $\mathbb{Z}_p$ is a finite field.

Ex

$\mathbb{Z}_2$ field

$\mathbb{Z}_3$ field

$\mathbb{Z}_4$ not(!) a field: $2 \cdot 2 = 0$.

$\mathbb{Z}_5$ field.

what a four-element field?

- None of the rings $\mathbb{Z}_N$ does this!
- But: $\{0, 1, \alpha, \alpha+1\}$.

compute modulo 2

0	0	0	0
0	1	α	$\alpha+1$
0	α	$\alpha+1$	1
0	$\alpha+1$	1	α

and $\alpha^2 + \alpha + 1 = 0$.

Fact: Whenever q is a power of a prime then there exists an (essentially unique) field $\mathbb{F}_q$ with q elements.

Chinese Remainder Theorem

Info 16.10.07 (13)

Teacher tries to line up his class in rows.

of three: one remains.

of four: two remain.

of five: that works; none remains.

Q: How many pupils did that teacher have? 10 or 70.

Denote by x the number of pupils.

Thus

$$\left.\begin{aligned} x \bmod 3 &= 1, \\ x \bmod 4 &= 2, \end{aligned}\right\}$$
$$x \bmod 5 = 0$$

3 and 4 are coprime.

We can thus run EEA and obtain

$$1 = \underbrace{s \cdot 3}_{=: x_1} + \underbrace{t \cdot 4}_{=: x_2}.$$

then $x_1 \bmod 3 = 0$, $x_1 \bmod 4 = 1$ | $x_2 \bmod 3 = 1$, $x_2 \bmod 4 = 0$

$$x = 1 \cdot x_2 + 2 \cdot x_1 \; ! \qquad \left.\begin{aligned} x \bmod 3 &= 1 \\ x \bmod 4 &= 2 \end{aligned}\right\} \Leftrightarrow x \bmod 12 = 10 \; (\equiv -2)$$

Here: $s = -1$, $t = 1$: $x_1 = -3$, $x_2 = 4$. $x = -2 + 12k$.

Repeating this:

$$x \bmod 12 = 10,$$
$$x \bmod 5 = 0.$$

Ex

$$1 = \overbrace{s' \cdot 12}^{x_1'} + \overbrace{t' \cdot 5}^{x_2'}$$

$s' = -2, \quad t' = 5$ by EEA.

So $x_1' = -24$ $\quad x_1' \bmod 12 = 0, \quad x_1' \bmod 25 = 1$

$x_2' = 25$ $\quad x_2' \bmod 12 = 1, \quad x_2' \bmod 25 = 0$

Put $x := 10 \cdot x_2' + 0 \cdot x_1'$

$= 250$

modulo $12 \cdot 5 = 60$

so $x \bmod 60 = 10.$

Chinese Remainder Theorem

Given $m_1, m_2, \dots, m_k \in \mathbb{N}_{\geq 2}$,
$\gcd(m_i, m_j) = 1$ for $i \neq j$.

Let $N = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Then $\mathbb{Z}_N \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$

$a \bmod N \longmapsto (a \bmod m_1, a \bmod m_2, \dots, a \bmod m_k)$

is well-defined, homomorphic, surjective!, injective

for short: it is an isomorphism.
(renaming!)

△

Corollary Suppose $N = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ with the (m_i) pairwise coprime.

Then
$$\mathbb{Z}_N^\times \cong \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \ldots \times \mathbb{Z}_{m_k}^\times$$

in particular:
$$\#\mathbb{Z}_N^\times = \#\mathbb{Z}_{m_1}^\times \cdot \#\mathbb{Z}_{m_2}^\times \cdot \ldots \cdot \#\mathbb{Z}_{m_k}^\times$$
$$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \|$$
$$\varphi(N) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_k)$$

Ex $\varphi(6) = \varphi(2) \cdot \varphi(3)$ since $2, 3$ are coprime

$$\varphi(4) \neq \varphi(2) \cdot \varphi(2) = 1 \cdot 1 = 1$$
$$\|$$
$$\#\mathbb{Z}_4^\times = 2 \qquad \mathbb{Z}_4^\times = \{\not{X}_{\checkmark 1}, \not{X}_{\checkmark -1}\}$$

$$\varphi(2) = \#\mathbb{Z}_2^\times = 1$$

Fact $\varphi(p^e) = (p-1)\, p^{e-1}$ for p prime

CRT ⇒ $\varphi(p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}) = (p_1-1)p_1^{e_1-1} \cdot \ldots \cdot (p_k-1)p_k^{e_k-1}$ for $p_1, \ldots, p_k$ different primes

Ex $\varphi(4) = (2-1)\cdot 2 = 1 \cdot 2 = 2.$

$\varphi(3^5) = (3-1)\cdot 3^4 = 2 \cdot 3^4.$

$\#\mathbb{Z}_p^\times = p-1$ since $\mathbb{Z}_p$ is a field or since ...

Simple Corollary p prime: $\varphi(p) = p-1$.

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$$
for p, q prime, $p \neq q$

RSA – 1.

Ex

$$x \bmod 7 = 1$$
$$x \bmod 9 = 2$$
$$x \bmod 10 = 3$$

Find x

Ex!

Prove that RSA is correct if $x \in \mathbb{Z}_N^\times$.

Ex

Compute $3^{98746530^1}$ in $\mathbb{Z}_{101}$.

Ex

Send mail to

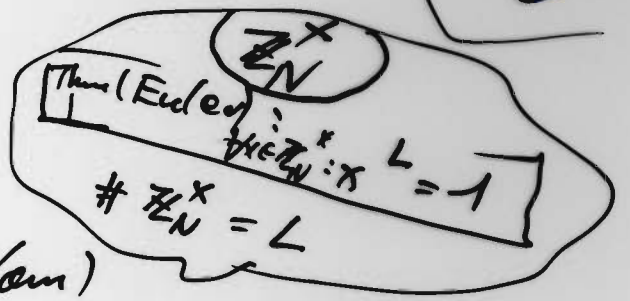
rueskeu@bit.uni-bonn.de

→ RSA is correct → Polynomials

→ RSA toy example

→ Summary

ZiCo 17.10.07 (1)



RSA toy example

$p = 23$ $q = 31$ (random)

$N = p \cdot q = 713$

$L = (p-1)\cdot(q-1) = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$

repetition Euclid

$d = 7 \in \mathbb{Z}_L^\times$ (random)

$e = ?$ s.t. $ed = 1$ in $\mathbb{Z}_L$.

EEA (L, d)

660		0	1
7	94	1	0
2	3	-94	1
1	2	283	-3
0		-660	7

Check: ✓

Output: $1, 283, -3$: $1 = 283 \cdot 7 + (-3) \cdot 660$

Thus $e = 283$.

Public key : $(N, e) = (713, 7)^{283_{\mathbb{Z}}}$,

Private key : $(N, d) = (713, 283)_{7_{\mathbb{Z}}}$.

Forget p, q, L.

Boi Co
17.10.07
(2)

Encrypt $x = 2$

$y = x^e$ in $\mathbb{Z}_N$

$e = 283 = 100011011_2$

$N = 713$

$2^1 = 2$

$2^{10} = 4$

$2^{100} = 16$

$2^{1000} = 256$

$2^{10000} = 653 = -60$

$2^{10001} = -120$

$2^{100010} = 140$

$2^{100011} = 280$

$2^{1000110} = -30$

$2^{10001100} = 187$

$2^{10001101} = 374$

$2^{10001010} = 128$

$2^{10001011} = 256 = y$

$65536 = 91 \cdot 713 + 653$

$= 92 \cdot 713 - 60$

$14400 = 20 \cdot 713 + 140$

$78400 = 109 \cdot 713 + 683$

$= 110 \cdot 713 - 30$

$900 = 1 \cdot 713 + 187$

$374^2 = 139\,876 = 196 \cdot 713 + 128$

In practice it must be larger!

Decrypt $y = 256$

$z = x^d$ in $\mathbb{Z}_N$ $\quad d = 7 = 111_2$

$N = 713$

$256^{10} = -60$

$256^{11} = -387$

$256^{110} = 39$

$256^{111} = 2 = z$

$-15360 = ? \cdot 713 + -387$

$387^2 = 149\,769 = ? \cdot 713 + 39$

$39 \cdot 256 = 9984 = ? \cdot 713 + 2$

Thm RSA is correct.

Pf We have to prove that for every

$x \in \mathbb{Z}_N$: $\quad y = x^e$ in $\mathbb{Z}_N$,

$z = y^d$ in $\mathbb{Z}_N$,

then $z = x$.

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

$= x^{ed}$.

We know that $ed = 1$ in $\mathbb{Z}_L$.

By CRT it is enough to show

→ that $x^{ed} = x$ in $\mathbb{Z}_p$

and $x^{ed} = x$ in $\mathbb{Z}_q$.

(The CRT tells us that $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$.)

We know that $ed = 1 + k \cdot L$ in $\mathbb{Z}$.

By the little Fermat theorem we have

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

in case $x \in \mathbb{Z}_p^\times$. (I.e. $x \neq 0$ in $\mathbb{Z}_p$, i.e. $p \nmid x$.)

Thus $x^{k(p-1)(q-1)} = 1$ in $\mathbb{Z}_p$

and $x^{ed} = x^{1+kL} = x$ in $\mathbb{Z}_p$.

This is also true for $x = 0$ in $\mathbb{Z}_p$.

In total: $x^{ed} = x$ in $\mathbb{Z}_p$.

Similarly: $x^{ed} = x$ in $\mathbb{Z}_q$ $\Rightarrow x^{ed} = x$ in $\mathbb{Z}_N$. □

BiCo
17.10.07
(4)

Summary

- RSA as a guiding example
  - Ring of integers modulo N
    addition, multiplication, ~~inverses~~
    partial inversion
  - Lagrange, Euler, Fermat
  - Square and multiply
  - Extended Euclidean Algorithm
  - Chinese Remainder Theorem
- RSA is correct and efficient

Polynomials

- 2^x No, $x^{4.2}+7$ No, $\sqrt{x^7+1}$ No,
  x^5+x+1 Yes!

A polynomial is a sum of products of one (or more) variables and constants from some {comm.} ring or field.

Example $1 \in \mathbb{Z}_2$. Then 1 is a polynomial over $\mathbb{Z}_2$
Or $x^2+x+1 \in \mathbb{Z}_2[x]$ is a polynomial over $\mathbb{Z}_2$.

$$(x^2+x+1)\cdot(x^3+1) = x^5+x^4+x^3+x^2+x+1.$$

Afi: $\mathbb{Z}_2[x]$ is a comm. ring. DO PANIC & PANC.

Division with remainder for polynomials over a field, say $\mathbb{Z}_2$.

$$x^6 + x^4 + x^2 + 1 = (x^3 + 1)(x^3 + x + 1) + x^2 + x$$

$$-(x^6 + x^4 + x^3)$$

$$x^3 + x^2 + 1$$

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

$$x^2 + x$$

Whenever $a, b \in \mathbb{Z}_2[x]$, $b \neq 0$

then there exist $q, r \in \mathbb{Z}_2[x]$

such that

$$a = q \cdot b + r$$

and

$$\deg(r) < \deg(b)$$

$\lceil \deg(0) = -\infty. \rfloor$

We can compute "modulo $x^3 + x + 1$", say:

we get the

ring of polynomials over $\mathbb{Z}_2$

modulo $x^3 + x + 1$:

$$\mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle = \mathbb{F}_8$$

$x^3 + x + 1 \,|_{x=0} = 1 \neq 0$
$x^3 + x + 1 \,|_{x=1} = 1 \neq 0$
$\Rightarrow \ldots \Rightarrow$ $x^3 + x + 1$ has no nontrivial factors; like a prime! irreducible

Elements of $\mathbb{F}_8 := \mathbb{Z}_2[x] / \langle x^3+x+1 \rangle$:

$0, 1, x, 1+x,$

$x^2, x^2+1, x^2+x, x^2+x+1$

Ex $x^3 = x+1$ in $\mathbb{F}_8$.

$$x^3 = 1 \cdot (x^3+x+1) + (x+1)$$

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

$$x+1$$

For AES the field $\mathbb{F}_{2^8} = \mathbb{F}_{256}$ is used and defined as

$$\mathbb{Z}_2[x] / \langle x^8 + x^4 + x^3 + x + 1 \rangle$$

Ex $x \bmod 7 = 1$ ✓

$x \bmod 9 = 2$ ✓

$x \bmod 10 = 3$ ✓

Find x

$x = 533 \bmod 630$

$\mathbb{Z}_{630} \overset{CRT}{\cong} \mathbb{Z}_7 \times \mathbb{Z}_9 \times \mathbb{Z}_{10}$

Ex! Prove that RSA is correct if $x \in \mathbb{Z}_N^*$.

Ex Compute $3^{98746531}$ in $\mathbb{Z}_{101}$.

101 prime, Little Fermat $\Rightarrow 3^{100} = 1$ in $\mathbb{Z}_{101}$

$\rightarrow 3^{\dots 01} = 3^1 = 3$ -11-

Ex Send mail to

nvesken@bit.uni-bonn.de

Ex

Divide $x^7 + x^4 - 1$

by $x^3 + x + 1$

over $\mathbb{Z}_3$.

Ex opt

Run another toy example for RSA

Ex

Consider the following game:

There is a circle of n light bulbs.

You can switch any 3 adjacent ones.

Someone left a single bulb burning.

Turn it off!

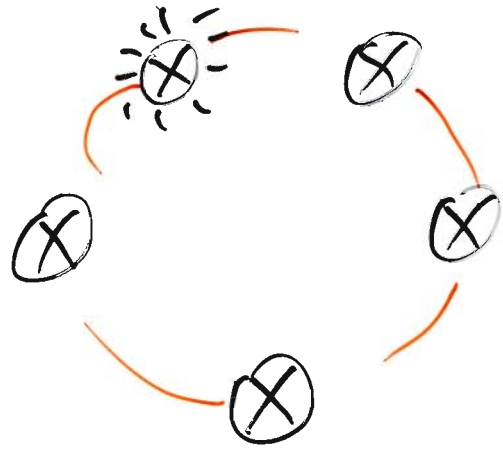
(a) case $n = 3$

(b) case $n = 4$

(c) case $n = 5$

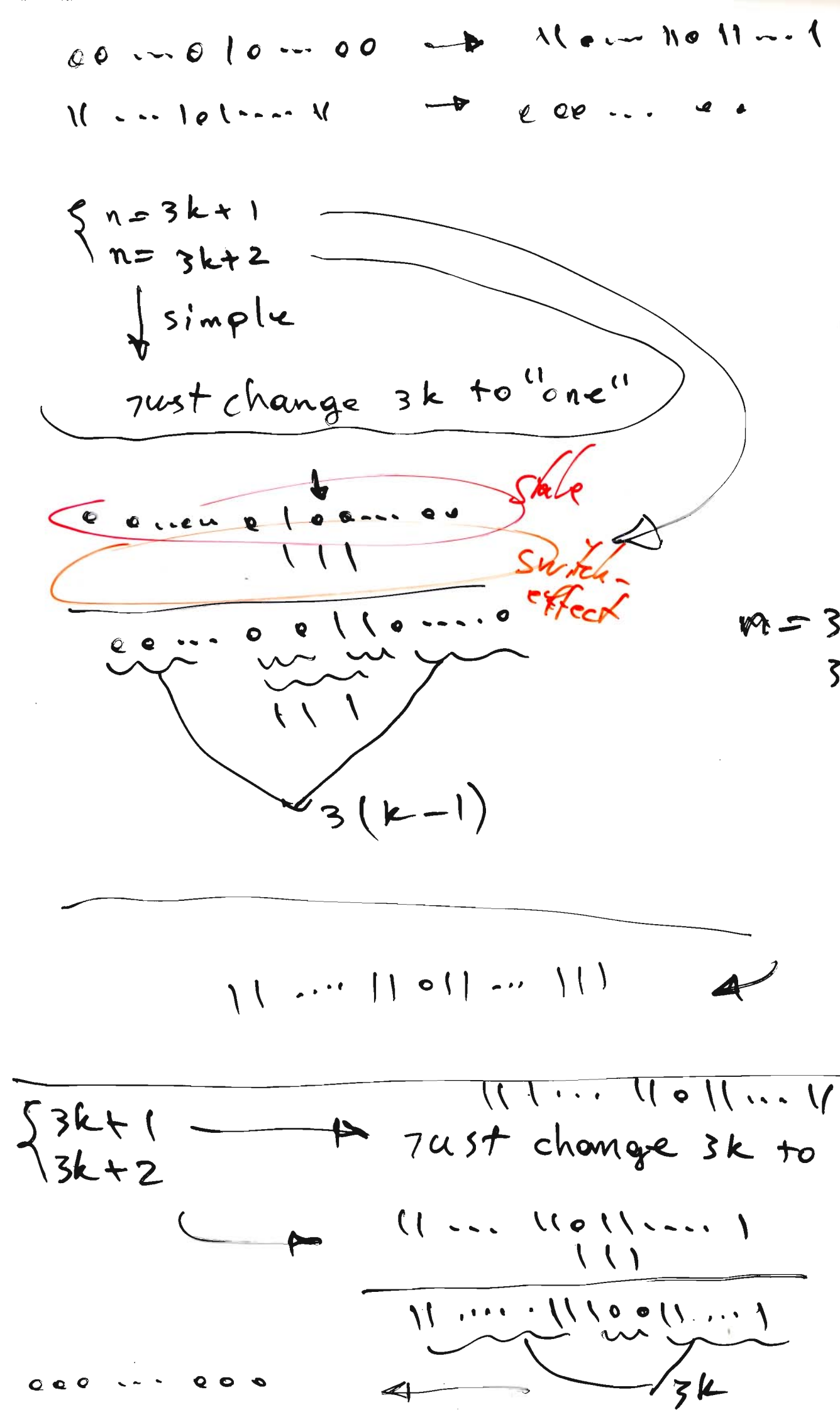
(d) case $n = 7$

(e) case $n = 11$



Find a procedure!

Hint: $1+1=0$ somewhere...


n = 3k+1
n = 3k+2
simple
just change 3k to "one"
stable
switch-effect
n = 3k+1
3k+2
3(k-1)
just change 3k to "zero"
3k

$n = 3$

State of the bulbs is
a string of three bits.
We start with $(1, 0, 0) =:$ state A.
If we switch: $+1\ +1\ +1$
we get $(0, 1, 1) =:$ state B
If we switch again
we get state A again.

$n = 6$?

Not immediate.

We make a mathematical model:
We describe the state of all bulbs
by a vector of n numbers in $\mathbb{Z}_2$.
We describe the effect of each switch
as such a vector:

$$s_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i \qquad s_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \leftarrow 0 \qquad s_{n-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix} \leftarrow n-1$$

Task: combine these into a state change $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

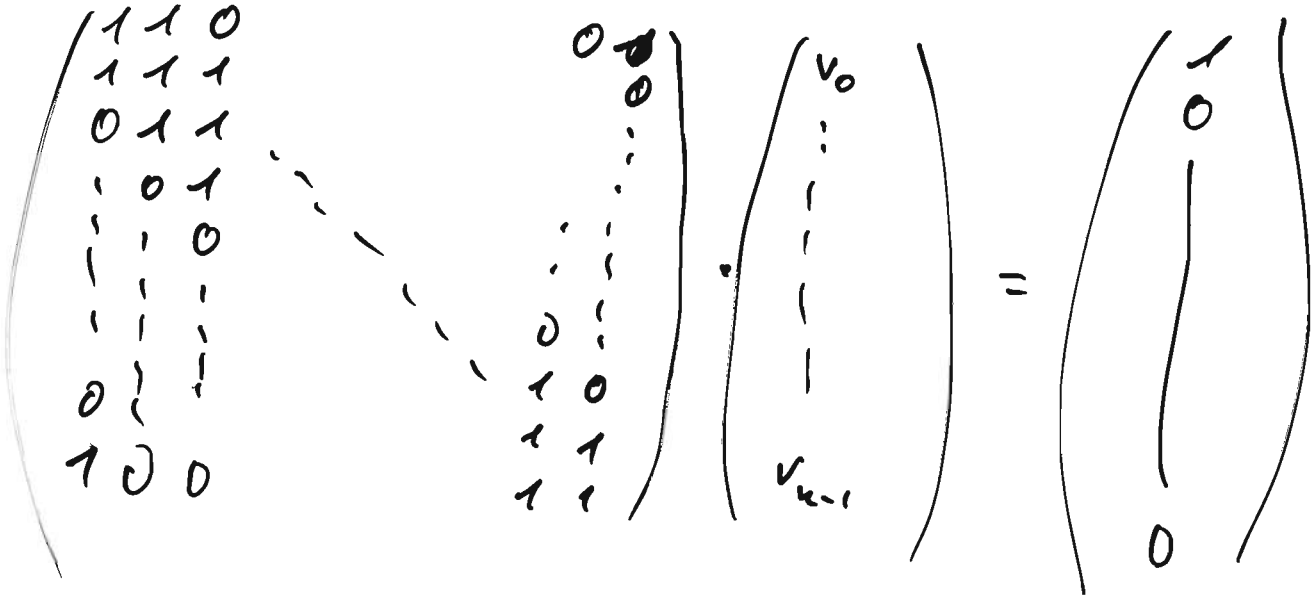
BriCo
17.10.07
(11)

So we look for a vector

$$v = (v_0, \dots, v_{n-1})^T$$

where v_i describes whether we operate switch i.

That is: solve that



over $\mathbb{Z}_2$.

$n = 3$:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Answer 1: No solution because: $v_0 + v_1 + v_2 = 1$ $\not\Rightarrow$ $v_0 + v_1 + v_2 = 0$

cannot be solved simultaneously.

Answer 2: No solution. Because:

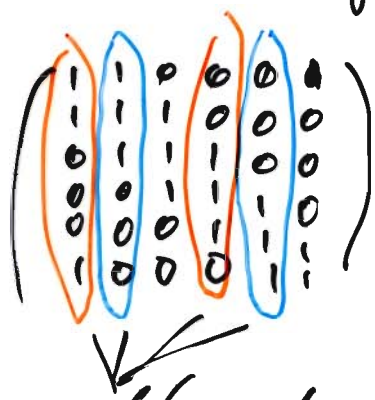
if we had a solution, then for every right hand side we could find a solution.

This is the case if and only if the determinant of our (square!) matrix is non-zero.

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 1 \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + 1 \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$= 1 \cdot 0 - 1 \cdot 0 + 1 \cdot 0 = 0$$

n=6 Answer works again:



$\det(\ldots) = 0$

add up to $\begin{pmatrix}0\\\vdots\\0\end{pmatrix}$ i.e. $(\ldots)\cdot\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}\vdots\\0\\\vdots\end{pmatrix}$ $\neq 0$

Thus our matrix is not invertible.

General Goal:

- Gauß algorithm
  "Good for numerics"
- Gauß-Jordan algorithm
  "Good for proofs"

$\mathbb{Z}_7^\times$	0	±1	±2	±3
$1/x$	–	±1	∓3	∓2

(Ex) Solve over $\mathbb{Z}_7$

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

(Ex) Solve over $\mathbb{Z}_{11}$

$$\begin{pmatrix}0 & 1 & 5\\ 3 & 0 & -1\\ 1 & 0 & 3\end{pmatrix} x = \begin{pmatrix}1\\3\\5\end{pmatrix}$$

If you know use each of the above algorithms once.

The Gaussian elimination in example 1

BiCo 18.10.07 (1)

$$\begin{pmatrix} 1 & 2 & 0 \\ -1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix} x = \begin{pmatrix} -1 \\ 0 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \text{ in } \mathbb{Z}_7$$

$\mathbb{Z}_7$ ∋ x	1	2	3
x^{-1}	1	−3	−2

1	2	0	−1	1
−1	3	1	0	0
0	1	2	3	0

1	2	0	−1	1
0	5	1	−1	1
0	1	2	3	0

5 = −2

← divide by 5, i.e. multiply by 3

1	2	0	−1	1
0	1	3	−3	3
0	0	−1	−1	−3

1	2	0	−1	1
0	1	3	−3	3
0	0	1	+1	+3

Done.

Conclusion: there exists a solution whatever right hand side there is, because we have no zero row in the matrix now.

So: $x_3 = 1$

$x_2 = -3 - 3x_1 = 1$

$x_1 = -1 - 2x_2 - 0x_3 = -3 = 4$

The Gauß-Jordan algorithm in example 1

$$\det = ?$$

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

multiply by 3

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

multiply by -1.

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

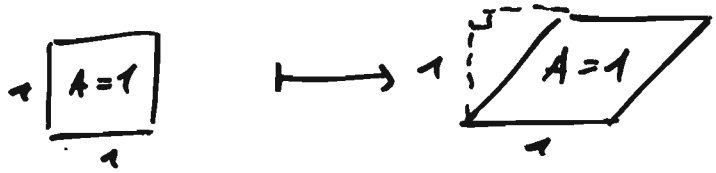
$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & -3 & -1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 3 \end{array}\right)$$

$$\det = \frac{1}{-3} = 2$$

$$= 1 \cdot (-2) \cdot (-1)$$

Solution: exists and $x = \begin{pmatrix} -3 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}$

	Effect on determinant
• Swap two rows.	Change sign.
• Scale a row by a constant	Multiply by that constant.
• Add a multiple of a row to another one.	None



Solve in this case:

$$\begin{pmatrix} 1 & 2 & 3 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} x = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Bsp 6
18.10.07
(3)

in $\mathbb{Z}_7$

$1^{-1} = 1$
$2^{-1} = -3$
$3^{-1} = -2$

$$\left(\begin{array}{cccccc|cc} 1 & 2 & 3 & 0 & 3 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{cccccc|cc} 1 & 2 & 3 & 0 & 3 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

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

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

row echelon form

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

Here: first right side allows many solutions, second right hand side allows <u>no</u> solution.

Describe all solutions! after Gauß-Jordan

BriCo 18.10.07 (4)

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

"entzerren"

Now any solution is of the form

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 3 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 2 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \end{pmatrix}$$

shows a lot of structure! It is an "affine space".

test with known form:

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

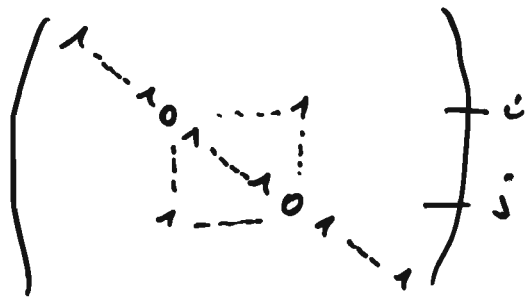
test with old form:

$$\begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

BriCo
18.10.07
(5)

Remark row operations as matrix multiplications *!**

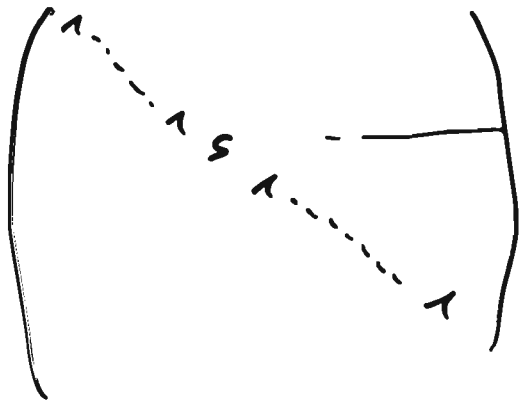
- Swap two rows

$P_{ij} =$ 

Now, if A' is the matrix we get from a matrix A by swapping row i and row j then

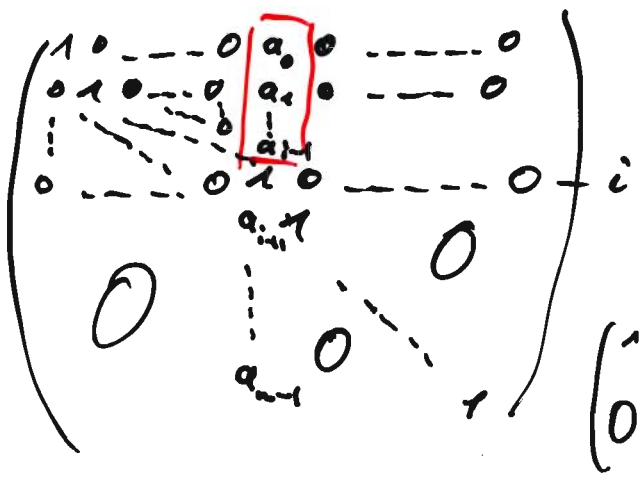
$$A' = P_{ij} \cdot A .$$

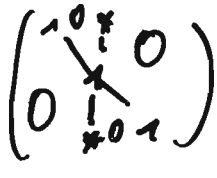
- Scale a row by a non-zero constant s

$S_{i,s} =$ 

if A'' is A with row i scaled by s, then $A'' = S_{i,s} \cdot A$.

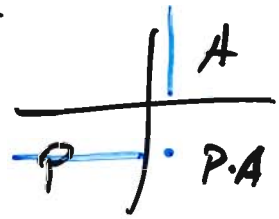
- Add a row to other rows

$A_{i,(a_0 \dots a_{n-1})} =$ 



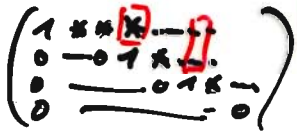
if row i is added a_j times to row j for $j \neq i$ then $A''' = A_{i,s} \cdot A$.

*



Thm

After Gauß elimination we arrive at a matrix R in 'weak echelon form'



[in square case: upper right triangular]

and it is related to the input matrix A by an equation $R = Q \cdot A$ with an invertible square matrix Q.

Actually, Q^{-1} is lower left triangular, (in case no swaps) occured, so that

$$P \cdot A = L \cdot R.$$

with $Q^{-1} = L$; with P a permutation matrix

To solve $Ax = b$ now solve $Ly = b$ and $Rx = y$

back substitution.

what happens to rhs during Gaußian elimination.

If you need Q then work on $A \mid 1\!\!1$, you'll get $R \mid Q$ at the end.

Run time?

Computing determinant using 'development along columns or rows' or using the formula $\det A = \sum_{\pi} (-1)^{\text{signature}} \prod a_{i,\pi(i)}$. needs $n!$ multiplications in the field.

$n! \in \Omega(2^n)$

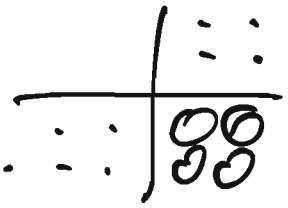
The Gaußian elimination or Gauß Jordan use $O(n^3)$ field operations.

Zürich 18.10.07 (6)

** Extra info:

Strassen (~1970)

Gaußian elimination
is not optimal.



Multiply 2×2 matrices:
usually you need 8 multiplications.

But it can be done with 7
without changing order of factors.

This leads to a recursive algorithm
which uses only $O(n^{\log_2 7})$ operations

for $n \times n$-matrices. $\ll O(n^{2.85})$

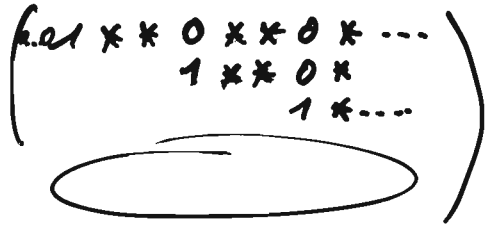
Current record: $O(n^{2.38})$ Coppersmith,
Winograd.

This also implies a similarly fast
algorithm for Gaußian elimination
(and also for the Gauß Jordan algorithm).

BriCo
18.10.07
(8)

Thm After the Gauß-Jordan algorithm we arrive at a matrix $\hat{R}$ in row 'echelon form'

and we'll have



$$R = Q \cdot A$$

with an invertible matrix Q.

To solve $Ax = b$ it is enough to solve $Rx = Qb$. [$QAx = Qb$.]

You have to perform a matrix-vector product and a 'back substitution' to get the solution for another b.

Runtime: $O(n^3)$ [or $O(n^{2.38}) \ldots$].

Structural questions:

- How does the set of solutions look like?
- When do solutions exist?
- How many solutions exist — in suitable sense?
- ~~When do solutions exist?~~
- When are solutions unique?

Suppose the row echelon form of our matrix A is this:

$$R = \begin{bmatrix} 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{over } \mathbb{Z}_{11}.$$

Exist? Sometimes, actually $Ax=b$ is solvable whenever Qb is of the form $\begin{bmatrix} x \\ x \\ x \\ 0 \end{bmatrix}$, i.e. $b = Q^{-1}\begin{bmatrix} x \\ x \\ x \\ 0 \end{bmatrix}$!

Unique? No, (with no rhs.)

→ How many? 2 parameters!

(One for each column without a 'pivot element'.)

Thus there are either no or $11^2 = 121$ solutions.

Dimension of the set of solutions,

$$\dim \{ x \mid Ax = 0 \} = 2.$$

For how many rhs-s b do we have solutions? $\{Q^{-1}\begin{bmatrix} x \\ x \\ x \\ 0 \end{bmatrix}\}$

In our example: 3 parameters!

$$\operatorname{rank} A := \operatorname{rank} R = \dim \underbrace{\{ b \mid \underbrace{b = A \cdot x \text{ for some } x}_{\text{image } \{ \text{im } A := \}} \}}_{''}$$

Repeat:

$$\begin{aligned} \operatorname{rank} A &:= \dim \operatorname{im} A \\ &= \operatorname{rank} R \\ &= \#\text{ non-zero rows in } R \\ &= \#\text{ pivot elements} \end{aligned}$$

and

$$\dim \underbrace{\{x \mid Ax = 0\}}_{=: \ker A} = \#\text{columns of } A - \#\text{ pivot elements.}$$

kernel

Together:

$$\underbrace{\dim \ker A}_{\text{"dim of the set of solutions}} + \underbrace{\dim \operatorname{im} A}_{\text{"rank}(A)} = \#\text{cols of } A.$$

□

$$\operatorname{im} A = \{ Ax \mid x \},$$

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

(Ex) Compute the row echelon form of the matrix

$$A = \left[\begin{array}{cccc|c} 2 & 1 & 3 & 0 & 3 \\ 0 & 0 & 4 & 2 & 0 \\ 2 & 1 & 0 & 2 & 3 \\ 0 & 0 & 0 & 1 & 5 \end{array}\right]$$

over $\mathbb{Z}_7$

and determine its rank and the dimension of the set of solutions. Describe the set (using parameters).

$\mathbb{Z}_7$: $2^{-1} = -3$, $3^{-1} = -2$.

Info
18.10.07
(11)

$$\begin{array}{ccccc} 2 & 1 & 3 & 0 & 3 \\ 0 & 0 & 4 & 2 & 0 \\ 2 & 1 & 0 & 2 & 3 \\ 0 & 0 & 0 & 1 & 5 \end{array}$$

↰ multiply by -3

$$\begin{array}{ccccc} 1 & -3 & -2 & 0 & -2 \\ 0 & 0 & -3 & 2 & 0 \\ 0 & 0 & -3 & 2 & 0 \\ 0 & 0 & 0 & 1 & 5 \end{array}$$

multiply by 2

$$\begin{array}{ccccc} 1 & -3 & 0 & -1 & -2 \\ 0 & 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 5 \end{array}$$

↰ swap
↲ multiply by 1

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

$$\text{So } R = \begin{bmatrix} 1 & -3 & 0 & 0 & 3 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} \begin{matrix} \\ 1 \\ -2 \end{matrix}.$$

i.e. $\operatorname{rank} A = \operatorname{rank} R = 3$

$\dim \ker A = 2$

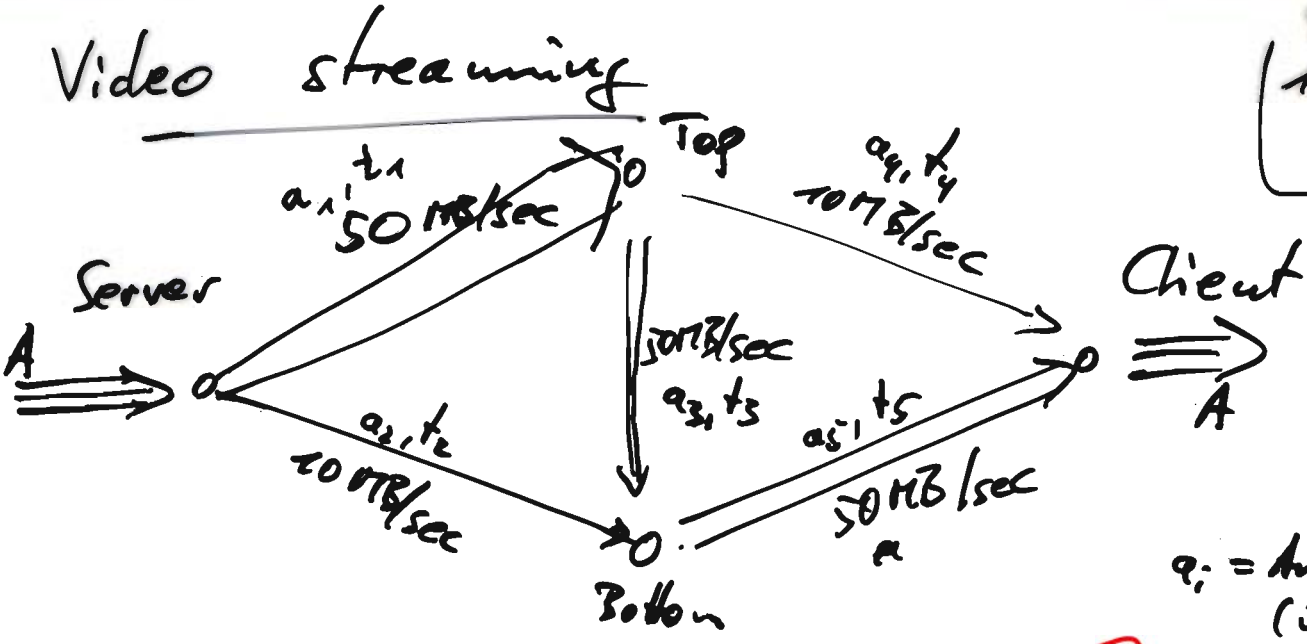
unabhängt R: $\begin{bmatrix} 1 & -3 & 0 & 0 & 3 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$

$\ker A$:

Hom: $0 + \lambda_1 \begin{bmatrix} -3 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 3 \\ 0 \\ 1 \\ -2 \\ -1 \end{bmatrix}$

is the set of solutions for $Ax = 0$.

Video streaming



a_i = Amount (in MB)

t_i = time

Conditions:

- At each node the (resulting) amount of data is zero, ie. everything received is sent away (later).

$$A = a_1 + a_2 \quad \text{(server)}$$

$$a_1 = a_3 + a_4 \quad \text{(Top)}$$

$$a_2 + a_3 = a_5 \quad \text{(Bottom)}$$

$$a_4 + a_5 = A \quad \text{(Client)}$$

- All packets use the same time:

$$t_1 + t_4 = T$$

$$t_2 + t_5 = T$$

$$t_1 + t_3 + t_5 = T$$

This is a linear system of equations. → Solve it!

- By definition:

$$a_1 = t_1 \cdot 50\ \text{MB/sec}$$

$$a_2 = t_2 \cdot 10\ \text{MB/sec}$$

$$\vdots$$

Guiding examples:

(I) Monty Hall problem

(II) Pollard-ρ

We start with N which is not prime (and not a prime power)

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

for example $f(x) = x^2 + 1$, assuming it to be random,

and a seed $x_0 \in_R \mathbb{Z}_N$, $y_0 := x_0$.

compute

$$x_{i+1} = f(x_i),$$

$$y_{i+1} = f(f(y_i)).$$

until $\gcd(x_{i+1} - y_{i+1}, N) \neq 1$.

$\gcd(x_{i+1} - y_{i+1}, N) = p$

Return p.

Heuristics: assume that the sequence $x_0, x_1, \ldots$ (uniformly) is completely chosen at random.

→ birthday paradox.

Turns out: heuristic expected runtime $O(\sqrt[4]{N})$

Birthday paradox: we need about $O(\sqrt{p})$ loop repetitions,

where p is the smallest prime factor of N, i.e. $p \leq \sqrt{N}$.

Thus we need about $O(\sqrt{N})$ repetitions.

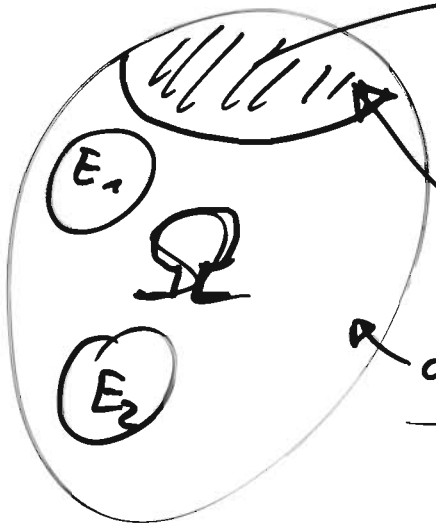
Much simpler

Consider the algorithm:

1. Repeat
2. something
3. Until Condition 17 holds

where $\text{prob}(\text{Condition 17}) = \frac{1}{42}$.

How many iterations of the loop do we expect?
In other words: what is the expected runtime?



X = Yes, it is beautiful!

$\text{prob}(X = \text{Yes}) = 0{,}15$ ← this is it's probability.

a part of it

anything that could happen

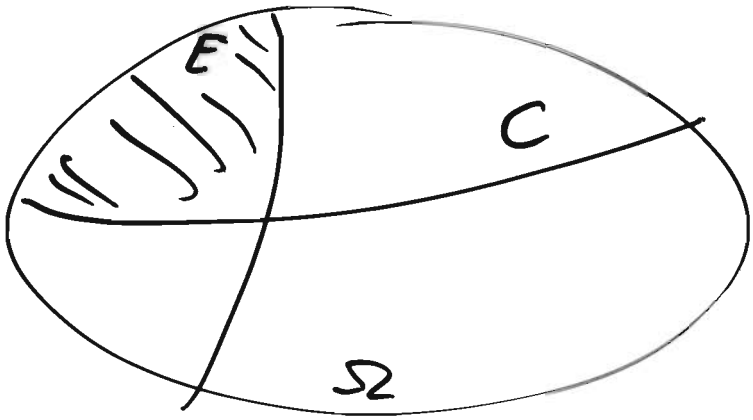
$\text{prob}(\text{Event}) \in [0,1] \subset \mathbb{R}$ $\quad E_1 \cap E_2 = \emptyset$

$\text{prob}(\emptyset) = 0$ $\quad \text{prob}(E_1 \dot\cup E_2) =$

$\text{prob}(\Omega) = 1$ $\quad \text{prob}(E_1) + \text{prob}(E_2)$.

$\text{prob}(\Omega \setminus E_1) = 1 - \text{prob}(E_1)$.

Conditional probabilities



We have:

$prob(E)$

$prob(C)$

$prob(E \cap C)$

$$prob(E \mid C) \quad \text{ii} \quad \frac{prob(E \cap C)}{prob(C)}$$

Random variable:

$$X : \Omega \longrightarrow \text{some set} =: \operatorname{im} X$$

so that we have the values

$$prob(X = x)$$

for $x \in \operatorname{im} X$.

Assume Ω finite

Good part of the story:

we can assume that any wanted random variable with prescribed values for $x \mapsto prob(X = x)$ exists.

distribution

BriCo 18.12.07 (15)

For our loop problem define

$$C_i = \begin{cases} 1 & \text{if condition 17 holds in the } i\text{-th repetition.} \\ 0 & \text{otherwise.} \end{cases}$$

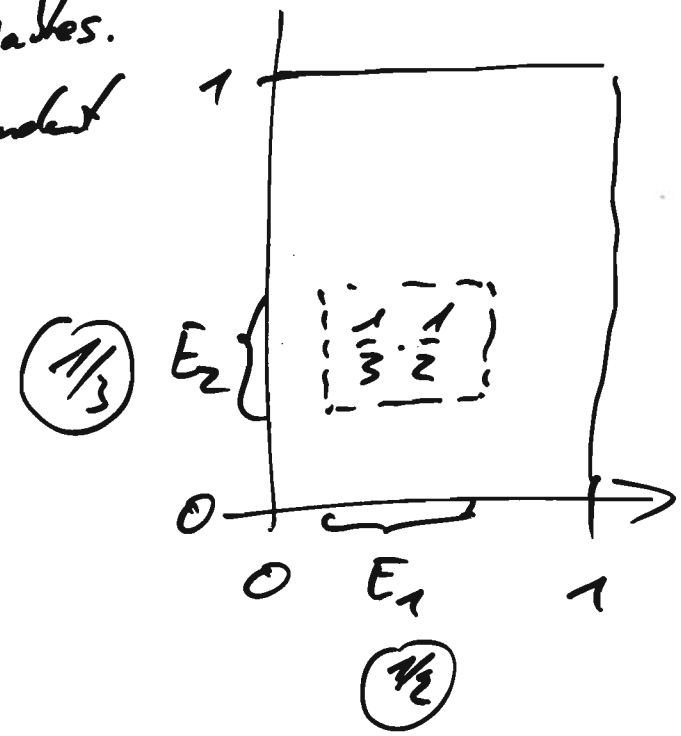
We know by assumption:

$$\text{prob}(C_i = 1) = \frac{1}{42}$$

and this is independent of all other C_j.

Def Let X, Y be random variables. Then we call (X, Y) independent if $\forall x \in \text{im}X, y \in \text{im}Y$:

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



We were in the middle of computing the runtime of the loop

1. Repeat
2. $x \in_R \mathbb{Z}_{42}$
3. Until $x = 0$ or 'huge' repetitions done

We have defined random variables

$$C_i = \begin{cases} 1 & \text{if } 'x=0' \text{ after round } i \\ 0 & \text{else.} \end{cases}$$

where $\text{prob}(C_i = 1) = p = \frac{1}{42}$,

and $\text{prob}(C_i = 1 \wedge (\underbrace{C_1 = 0 \wedge C_2 = 0 \wedge C_3 = 0 \wedge \ldots \wedge C_{i-1} = 0}_{***}))$

$= \text{prob}(C_i = 1) \cdot \text{prob}(\ldots)$.

[mathematical theory guarantees existence.]

We want to compute the expected runtime.

The runtime

$$T = \min\{ i : C_i = 1 \}$$

is also a random variable! with values in $\mathbb{R}$.

We want

$$E(T) = \sum_{t \text{ huge}} t \cdot \underbrace{\text{prob}(T = t)}_{?} + \text{huge} \cdot \underbrace{\text{prob}(T > \text{huge})}_{\text{fail until bound reached}}$$

$\leq$

In our example:

$$\text{prob}(T=t)$$

$$= \text{prob}(C_1=0 \wedge C_2=0 \wedge \dots \wedge C_{t-1}=0 \wedge C_t=1)$$

$$= \text{prob}(C_1=0) \cdot \text{prob}(C_2=0) \cdot \dots \cdot \text{prob}(C_{t-1}=0) \cdot \text{prob}(C_t=1)$$

$$= \underbrace{(1-\varrho)}_{=:\sigma} \cdot (1-\varrho) \cdot \dots \cdot (1-\varrho) \cdot \varrho$$

$$= \sigma^{t-1} \cdot \varrho .$$

so

$$E(T) = \lim_{\text{huge}\to\infty} \left(\sum_{t=1}^{\text{huge}} t \cdot \sigma^{t-1} \cdot \underbrace{(1-\sigma)}_{\varrho} + \text{huge} \cdot \sigma^{\text{huge}} \right)$$

$$= \varrho \underbrace{\sum_{t=0}^{\infty} t\, \sigma^{t-1}}$$

$$= \frac{d}{d\sigma} \left(\sum_{t=0}^{\infty} \sigma^t \right)$$

geometric series with factor σ, and whenever $|\sigma|<1$ then $\sum_{t\geq 0} \sigma^t = \frac{1}{1-\sigma}$

$$= \frac{d}{d\sigma} \left(\frac{1}{1-\sigma} \right)$$

$$= + \frac{1}{(1-\sigma)^2}$$

$$= \varrho \cdot \frac{1}{\varrho^2} = \frac{1}{\varrho} = 42 \; !$$

□

Another question:
back to Monty Hall.

Zilo
19.10.07
(3)

prob (Price is behind the door that the winner chose) = $\frac{1}{3}$.

LUCKY

Now, the quizz masters opens a losing door and the winner may revise his choice.

prob (LUCKY without changing | Door 3 loses and is opened by quizz master)

$\frac{1}{3}$

$= \frac{1}{2} =$ Prob (Door chosen wins | Door opened ≠ Door opened)

$= \frac{\text{prob (Door chosen is a Door chosen ≠ ...)}}{\text{prob (} \quad + \quad \text{)}}$

$= \frac{1/3}{2/3}$

That's it, right?

Bri'Co
19.10.07
(4)

Reinterpret the game:

The winner has two decisions:

(1) fix a door

(2) either: open one door (not changing)
or open all other doors (changing).

Thus prob(LUCKY without changing) = $\frac{1}{3}$,

prob(LUCKY with changing) = $\frac{2}{3}$.

BE AWARE OF INTERPRETATIONS!

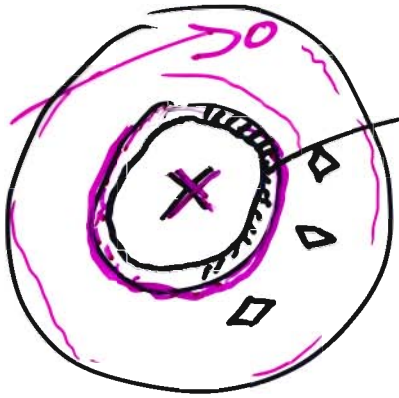
MODELS CAN BE MISLEADING!

BnCo
19.10.07
(5)

Ex

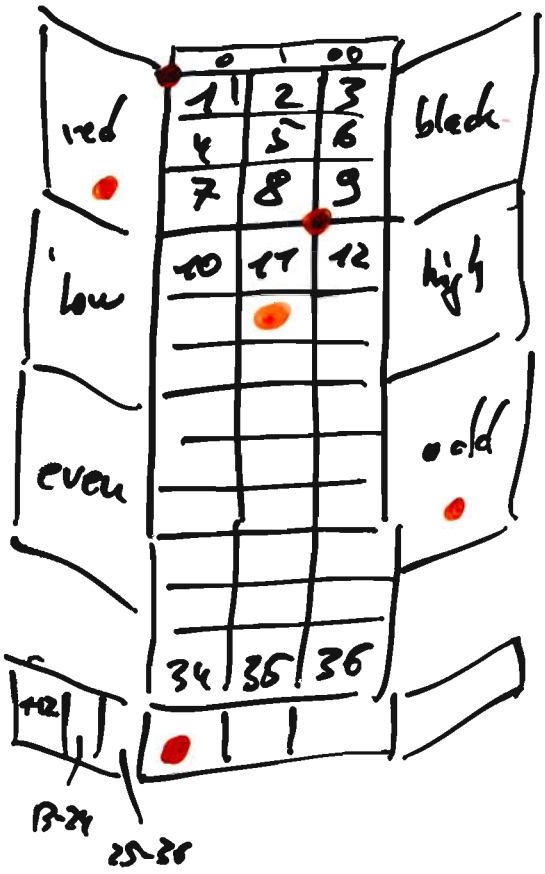
(i) What is the appropriate probability space (and distribution) for Roulette?

or a (set of) random variables with distribution



38 boxes
(37)

0, 00,
1, 2, 3, 4, 5, 6, 7, ...
36



You can bet

(a) on a single number
payoff: 36 × amount.

(b) on 'halfs'

even/odd } payoff
low/high } is
red/black } 2 × amount

but 0, 00 are in neither 'half'.

(c) on 'thirds'

What are the probabilities to win ↺?

(ii) What's the expected win (payoff − amount) if you bet on high?

(iii) What's the expected win if you keep doubling your bet, until you win first?

on high

Answers

BriCO 19.10.07 (6)

(i): Let X be a num r.v. with possible outcomes $0, 00, 1, 2, 3, \dots 36$ and

$$\text{prob}(X = x) = \frac{1}{38}$$

for all $x \in \{0, 00, 1, 2, 3, \dots, 36\}$.

(b) $\text{prob}(X \in \text{high}\}$ $\{X=17 \wedge X=18\} = \emptyset$.

$= \text{prob}(X=17) + \text{prob}(X=18) + \dots + \text{prob}(X=36)$

$= \frac{18}{38} =: \varrho < \frac{1}{2}$.

Payoff here is: 2x amount (not $\frac{38}{18}$ x amount!)

(ii) Consider the r.v. describing the win if we bet 1€ on high:

$$W = \begin{cases} 2€ - 1€ & \text{if } X \in \text{high} \\ -1€ & \text{otherwise} \end{cases}$$

$\text{prob}(X \in \text{high}) = \varrho$

$\text{prob}(X \notin \text{high}) = 1 - \varrho$

$-\frac{2}{38}$ €

$E(W) = 1€ \cdot \varrho + (-1€) \cdot (1-\varrho) = (2\varrho - 1) \cdot 1€$

ZiCo 19.10.07 (7)

(iii) X_i = a r.v. for the ith round in Roulette.

prob (first win is in round t)

$= prob(X_1 \notin high \wedge X_2 \notin high \wedge \dots \wedge X_{t-1} \notin high \wedge X_t \in high)$

$= prob(X_1 \notin high) \cdot \dots \cdot prob(X_{t-1} \notin high) \cdot prob(X_t \in high)$

$= \sigma \cdot \dots \cdot \sigma \cdot \varsigma \quad , \sigma = 1 - \varsigma .$

$= \sigma^{t-1} \varsigma$

prob(not win in t rounds) $= \sigma^t$.

$$W_\varepsilon = \begin{cases} 2^{\overbrace{i \text{ times}}^{\text{prior placements}}} - 2^{i-1} - 2^{i-2} - \dots - 2 - 1 & \text{if we win first in round } i \\ \vdots & \\ -2^{huge-1} - 2^{huge} - \dots - 2 - 1 & \text{if we never win in the first 'huge' rounds} \end{cases}$$

$$= \begin{cases} 1 & \text{if we win first in round } i \\ \vdots & \\ 1 - 2^{huge} & \text{if we lose until end.} \end{cases}$$

$\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$ for $x \neq 1$

$$E(W) = \sum_{i \le huge} 1\varepsilon \cdot prob(\text{first win is in round } i) + [1 - 2^{huge}]\varepsilon \cdot prob(\text{no win in huge rounds})$$

$E(W) = 1€ \cdot \underbrace{\sum \text{prob}}_{1}$

$-2^{\text{huge}}€ \cdot \sigma^{\text{huge}}$

$\sigma = \frac{20}{38} > \frac{1}{2}.$

$= 1€ - \underbrace{(2\sigma)}_{>1}^{\text{huge}}$

$2\sigma > 1.$
$\|$
$\frac{40}{38}$

If we let huge tend to infinity

then $E(W^{(\text{huge})}) \longrightarrow -\infty.$

IF YOU WANT TO BE SUCCESSFUL
IN GAMBLING THEN
EITHER: DON'T PLAY

OR

BE THE BANK,
& OPEN A CASINO.

BriCo
13.10.07

Ex (i) Set up a 'model' for rolling three dice and say X_1, X_2, X_3 are r.v. describing it. $\text{prob}(X_i = j) = \frac{1}{6}$; independent

(ii) What is the expected sum of the dice?

$E(X_1+X_2+X_3) = 10.5$

$= E(X_1) + E(X_2) + E(X_3)$

(iii) Calculate the probability that

(a) all three dice show the same number, $1/36$

(b) all three dice show different numbers. $\frac{1}{6} \cdot \frac{1}{5} \cdot \frac{1}{4}$

(iv) Calculate the conditional probability that the sum of the dice is even given that none shows a six. $\neq \frac{1}{2}$

Ex A car was involved in an accident. A

The brakes fail sometimes. B

We say, know:

$\text{prob}(B) = 0.01\%$

- the probability that the brakes fail is 0,01%.
- the probability that a car has an accident if the brakes fail is 60%. $\text{prob}(A|B) = 60\%$
- the probability that a car has an accident is 0.1%. $\text{prob}(A) = 0.1\%$

What is the probability that the brakes failed if the car had an accident?

$(A|B)$

$$\text{prob}(B|A) = \frac{\text{prob}(A \cap B)}{\text{prob}(A)} = \frac{\text{prob}(B)}{\text{prob}(A)} \cdot \text{prob}$$

EriCo
19.10.07
(20)

Summary

Probabilities (finite ...)
- Spaces and 'prob' function
- Random variables
- Simple basic rules
- Independent
- Applications: eg. average runtime of a probabilistic loop.

Linear Algebra
- Gaußian elimination
- Gauß-Jordan algorithm
- $\underbrace{\dim \ker A}_{\text{"size" of the set of solutions}} + \underbrace{\dim \operatorname{im} A}_{\operatorname{rank} A} = \#\text{cols}(A)$
- Existence of solutions, Uniqueness

Elementary Number Theory
- Extended Euclidean Algorithm
- Square and multiply (Repeated squaring) → fast exponentiation
- Fermat, Euler, Lagrange
- Chinese Remainder Theorem
- RSA
- ~~Integers~~ Ring of integers modulo N: $\mathbb{Z}_N$
- → Polynomials and 'larger' finite fields