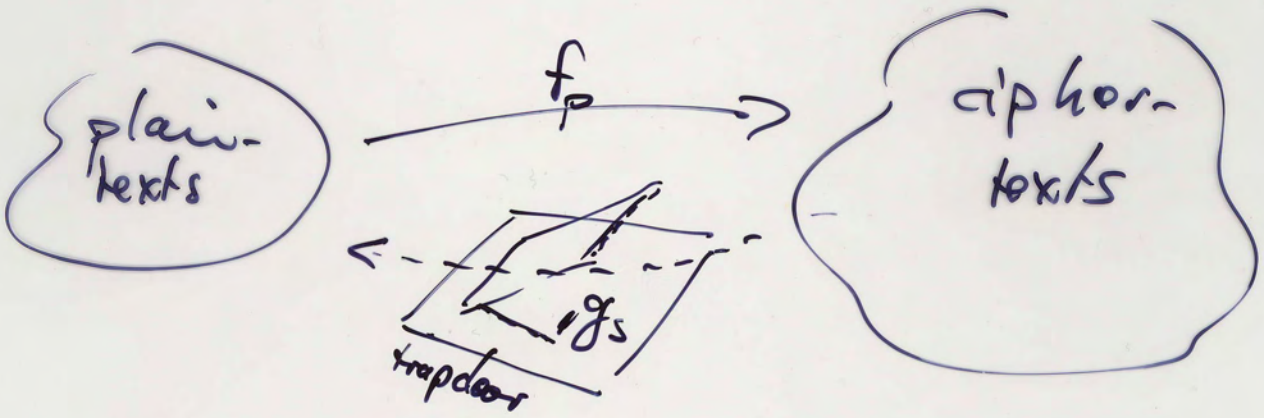


RSA
Rivest Shamir Adleman

178

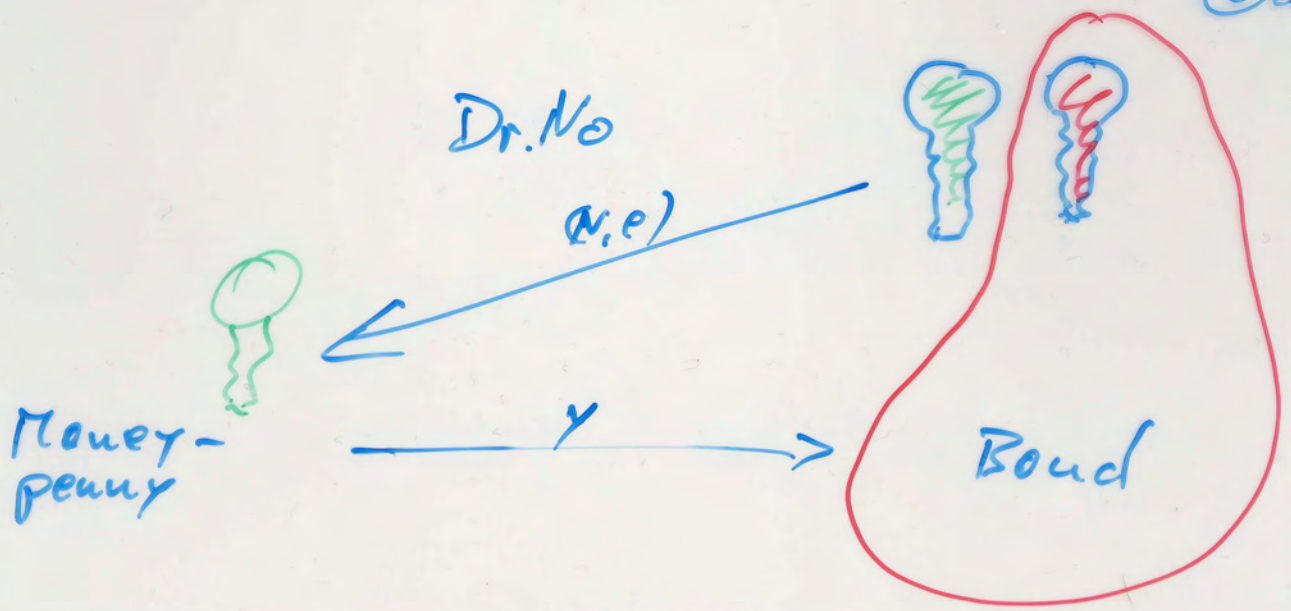
based on integer factorization

How does it work?

- Choose two primes p, q, $p \neq q$.
  and large and randomly.
- Let $N \leftarrow p \cdot q$, $L \leftarrow (p-1)(q-1)$.
- Choose two numbers $e, d \in \mathbb{N}_{<L}$,
  such that $e \cdot d \equiv 1$ modulo L.
  $ed = 1$ in $\mathbb{Z}_L$
  (Ie. $\frac{ed-1}{L} \in \mathbb{Z}$, $ed \operatorname{rem} L = 1$.
  L divides $(ed-1)$,
  $L \mid (ed-1)$.)
- Now: (N, e) is the public key,
  (N, d) is the secret key.

Throw away anything else!!!!!

- Suppose you encoded your message as a number $x \in \mathbb{N}_{<N}$. Encrypt it: $y \leftarrow x^e \operatorname{rem} N$.
- Decrypt it: $z \leftarrow y^d \operatorname{rem} N$.



---

class „ring of integers modulo N".

$\mathbb{Z}_N$

elements: $0, 1, 2, 3, \ldots, N-1$

operations:

$+ : \quad a +_{\mathbb{Z}_N} b := (a +_{\mathbb{Z}} b) \text{ rem } N$

$\cdot : \quad a \cdot_{\mathbb{Z}_N} b := (a \cdot_{\mathbb{Z}} b) \text{ rem } N.$

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

$- : \quad \ldots$

0

1

axioms

ring

commutative group (with +)

Proper: +, − are properly def'd.

Assoc. $(a+b)+c = a+(b+c)$

Neutral $a+0 = a = 0+a$

Inverses $a+(-a) = 0 = (-a)+a$

Commut. $a+b = b+a$

P: $\cdot$ is properly def'd

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

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

C: $a \cdot b = b \cdot a$

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

Thm $0 \cdot a = 0$.

Ex

Thm $0 \cdot a = 0$

Pf

$0 \cdot a \overset{N}{=} 0 \cdot (a+0)$

$\overset{D}{=} 0 \cdot a + 0 \cdot 0$ ($0 \cdot 0 = 0$ (Lemma!))

$a + (-a) = 0$

$(a + (-a)) \cdot b = a b + (-a) \cdot b$

$= a \cdot (b + (-b))$

$0 = a + (-a)$

$1 + (-1) = 0$ (b)

$0 \cdot a = (1 + (-1)) \cdot a$

$= 1 \cdot a + (-1) \cdot a$

$= a + (-1) \cdot a$

$a + (-a) = 0$

$0 + 0 \overset{N}{=} 0$

$(0+0) \cdot a \overset{D}{=} 0 \cdot a + 0 \cdot a$

$\| N$

$0 \cdot a$

$\| N$

$0 + 0 \cdot a$

$(0 + 0 \cdot a) + (-0 \cdot a) = (0 \cdot a + 0 \cdot a) + (-0 \cdot a)$

$\| A$ $\| A$

$0 + (0 \cdot a + (-0 \cdot a))$ $\quad 0 \cdot a + (0 \cdot a + (-0 \cdot a))$

$\overset{I}{=} 0$ $\quad \overset{I}{=} 0$

$\| N$ $\quad \| N$

0 $\quad 0 \cdot a$.

□

Examples

$4 \cdot 5 = 6$ in $\mathbb{Z}_7$

$\lceil 4 \cdot 5 = 20$ in $\mathbb{Z}$.

$20 = 2 \cdot 7 + 6$ (remainder!)

$2 \cdot 3 = 0$ in $\mathbb{Z}_6$

$4 \cdot 5 = -1$ in $\mathbb{Z}_7$ true

$b + b = b + 0$

$\Downarrow$

$b = 0$

Variation of the class

other element set: $-\left\lceil \frac{N-1}{2} \right\rceil, \dots, -1, 0, 1, \dots \left\lfloor \frac{N-1}{2} \right\rfloor$

$N = 7$: $-3, -2, -1, 0, 1, 2, 3$

$N = 4$: $-2, -1, 0, 1$

$\mathbb{Z} \xrightarrow{\text{mod}} \mathbb{Z}_N$

$a \longmapsto$ „a rem N“ $\in \mathbb{Z}$

4

$\mathbb{Z} \longrightarrow \mathbb{Z}_7$

4 $\longmapsto$ 4

$4 \cdot 4 = 16$ $\longmapsto$ $4 \cdot 4 = 2$

$\mathbb{Z} \times \mathbb{Z} \twoheadrightarrow \mathbb{Z}$

$(a, b) \longmapsto a$ rem b

$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}_b$

$(a, b) \longmapsto a \bmod b$

Multiplicative inverses

Example 2 in $\mathbb{Z}_7$.
What is x with $2 \cdot x = 1$?
Here, $x = 4$ is a solution: $2 \cdot 4 = 1$ in $\mathbb{Z}_7$.

$\mathbb{Z}_7$:

a	0	1	2	3	-3	-2	-1
a^{-1}	none	1	4 = -3	5 = -2	-5 = 2	-4 = 3	-1

Problem Given x in $\mathbb{Z}_N$.
Find y such that $x \cdot y = 1$ in $\mathbb{Z}_N$.

$\frac{-k \cdot N + 1}{x} = y$

Problem Given x in $\mathbb{Z}$, $N > 0$.
Find y and k in $\mathbb{Z}$
such that $y \cdot x + k \cdot N = 1$

Example $x = 2$, $N = 7$.

$1 \cdot 2 + 0 \cdot 7 = 2$ $\quad / \cdot (-3)$
$0 \cdot 2 + 1 \cdot 7 = 7$

$7 = 3 \cdot 2 + 1$

$(-3) \cdot 2 + 1 \cdot 7 = 1$

division with remainder

1015 : 15 = 67

90
113
105
8

$1013 = 67 \cdot 15 + 8$

quotient, remainder

quick division

running time: $O(n^2)$

Example $x = 142$, $N = 349$.

$$0 \cdot x + 1 \cdot N = 349$$
$$1 \cdot x + 0 \cdot N = 142$$
$$(-2) \cdot x + 1 \cdot N = 65$$
$$5 \cdot x + (-2) \cdot N = 12$$
$$(-27) \cdot x + 11 \cdot N = 5$$
$$59 \cdot x + (-218) \cdot N = 2$$
$$(-145) \cdot x + 59 \cdot N = 1$$
$$349 \cdot x + (-142) \cdot N = 0 \leftarrow \text{Verification}$$

$349 = 2 \cdot 142 + 65$

$142 = 2 \cdot 65 + 12$

$65 = 5 \cdot 12 + 5$

$12 = 2 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Extended Euclidean Algorithm

thus $142^{-1} = -145$ in $\mathbb{Z}_{349}$.

i	r_i	q_i	s_i	t_i
0	349		1	0
1	142	2	0	1
2	65	2	1	-2
3	12		-2	5
		⋮		

Example $x = 12, \quad N = 70.$

	i:	r_i:	q_i:	s_i:	t_i:
	0	70	-	1	0
	1	12	6	0	1
$\ell \to$	2	-2	-6	1	-6
	3	0		6	-35

We read off: $2 = \underbrace{(-1)\cdot 70 + 6 \cdot 12}_{\text{and no smaller result possible.}}$.

$\Rightarrow$ No inverse exists for 12 in $\mathbb{Z}_{70}$.

Theorem

(a) If the EEA finds a solution to $y \cdot x + k N = 1$ then we have $x^{-1} = y$ in $\mathbb{Z}_N$; inverse exists!

(b) If the EEA terminates without a solution, i.e. the last non-zero remainder is neither $+1$ nor -1, then (i) there is no solution, (ii) x has no inverse in $\mathbb{Z}_N$

Pf (a) is clear.

(b) ! If x and N have a common divisor d which is neither $+1$ nor -1, then $y \cdot x + k \cdot N$ is also divisible by d and thus $\neq 1$.

So suppose the EEA terminates with

$r_{\ell+1} = 0$ and $r_\ell = d = y \cdot x + k \cdot N \neq \pm 1$.

Note that $\boxed{r_{i-1} = q_i \cdot r_i + r_{i+1}}$ for $1 \le i \le \ell$

I Basis: $i = \ell$: $d \mid r_i$ and $d \mid r_{i+1}$.
$r_i = d$, $r_{i+1} = 0$ ✓

I Step: $i \to i-1$, $i \ge 1$:
We have $d \mid r_i$ and $d \mid r_{i+1}$.
We want $d \mid r_{i-1}$ and $d \mid r_i$.

$d \mid r_i \to d \mid q_i r_i$; $d \mid r_{i+1}$ $\Rightarrow d \mid \underbrace{q_i r_i + r_{i+1}}_{= r_{i-1}}$ ✓

I Concl: $d \mid r_i$ & $d \mid r_{i+1}$ for all $0 \le i \le \ell$. ✓ △

In particular: $d \mid r_0 = N$ and $d \mid r_1 = x$.
Thus we have a non-trivial common divisor of N and x. □

Remark
We also proved that the last non-zero remainder is the "greatest common divisor".

Pf We know $d \mid N$ and $d \mid x$, and $d = y \cdot x + k \cdot N$ for some y, k.
The other way round: suppose $c \mid N$ and $c \mid x$.
Then $c \mid y \cdot x + k \cdot N = d$.
I.e. d is a greatest common divisor. □

Wiederholung

- $\mathbb{Z}_p$ is always a field if p prime.

- **Fact:** If f is a polynomial over a field of degree k then f has at most k solutions/zeroes.

- **Thm** (Little Fermat) For $a \in \mathbb{Z}_p$, $a \neq 0$ we have $a^{p-1} = 1$ (in $\mathbb{Z}_p$).

If now $a^{\frac{p-1}{2}} \neq \pm 1$ then p was not prime!

Better: $p-1 = 2^e \cdot r$, r odd

$\frac{p-1}{2} = 2^{e-1} r$

Then $a^r, a^{2r}, a^{2^2 r}, \ldots, a^{2^{e-1} r}, a^{2^e r}$

(Squaring: $\neq 1$, $= 1$)

$\Rightarrow$ MILLER-RABIN-test

~~382~~

197

x

$x, x^2, x^3, x^4, x^5, x^6, \ldots, x^{197}$ 196 mult.

x^{13}

$x, x^2, x^4, x^8, x^{12}, x^{13}$ 5 mult (instead of 12!)

x^{197} $197 = (1100\,0101)$

(n)

$x, x^{10}, x^{11}, x^{110}, x^{1100}, x^{11000}, x^{110000}, x^{110001}$

$x^{1100010}, x^{11000100}, x^{11000101}$

10 mult. (instead of 196)

This needs at most $2(n-1)$ mult.

Thus exp. costs $O(n^3)$.

Thm

The EEA computes

(a) the greatest common divisor g of the input elements x and N

(b) integers s and t such that

$$g = s \cdot x + t \cdot N.$$

So either $g = 1$ (or $g = -1$) and $sx + tN = 1$

and $x^{-1} = s$ in $\mathbb{Z}_N$

$\leftarrow (x \bmod N)^{-1} = (s \bmod N)$

or $g \neq \pm 1$

and $g \mid x$ and $g \mid N$

and no solution of $sx + tN = 1$ exists

and no inverse of x in $\mathbb{Z}_N$ exists.

$\leftarrow x \bmod N$

Corollary

unit group of $\mathbb{Z}_N$

$$\mathbb{Z}_N^\times := \{ x \in \mathbb{Z}_N \mid \underbrace{\exists\, y \in \mathbb{Z}_N : yx = 1 \text{ (in } \mathbb{Z}_N)}_{x \text{ is invertible}} \}$$

$$= \{ \underbrace{]x[\bmod N}_{=: u} \mid]x[\in \mathbb{Z},\ 0 \le]x[< N,\ \underbrace{\gcd(]x[, N) = 1}_{\text{“}x \text{ coprime to } N\text{”}} \}$$

Pf Take $x \in \mathbb{Z}_N^\times$ ie. $\exists\, y \in \mathbb{Z}_N : y \cdot x = 1$.

Write $x = \underbrace{]x[}_{\in \mathbb{Z}} \bmod N$ and $y = \underbrace{]y[}_{\in \mathbb{Z}} \bmod N$

Now we know $]y[\cdot\,]x[+ k \cdot N = 1$ for some $k \in \mathbb{Z}$.

Thus the gcd of $]x[$ and N is 1.

Thus $x =]x[\bmod N \in U$.

Take $x \in U$, i.e. $x = [x] \bmod N$
with $[x] \in \mathbb{Z}$, $0 \leq [x] < N$,
and $\gcd([x], N) = 1$.

Thus the EEA will find $s, t \in \mathbb{Z}$ such that

$$1 \cdot [x] + t \cdot N = 1$$

and $x^{-1} = s \bmod N$ in $\mathbb{Z}_N$.

Ie. $x \in \mathbb{Z}_N^\times$. □

Example

$$\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, -7, -6, -5, -4, -3, -2, -1\}$$

$$\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, -7, -4, -2, -1\}$$

because $2 \cdot 8 = 1$
or $\gcd(2, 15) = 1$.

$3 \notin \mathbb{Z}_{15}^\times$ because $\gcd(3, 15) = 3 \neq 1$.

side remark: $1^2 = 1$, $(-1)^2 = 1$
and $4^2 = 1$, $(-4)^2 = 1$.
Thus $x^2 = 1$ has 4 solutions

Ex

$$\mathbb{Z}_{12}^\times = \{1, 5, -5, -1\}$$

$12 = 2^2 \cdot 3^1$

$2^1(2-1)\ 3^0(3-1) = 4$. ≠

Question

Consider an element x in $\mathbb{Z}_N$.

Compute the sequence

$$1, x, x^2, x^3, x^4, \dots$$

by multiplying with x to get a new element.

What special properties does the sequence have?

Ex $N = 6$, $x = 2$ in $\mathbb{Z}_6$.

$\#\mathbb{Z}_N^\times = 2$

$1, 2, 4, 2, 4, 2, 4, 2, 4, \dots$ period 2

$\cdot 2 \quad \cdot 2 \quad \cdot 2$

Observation: this sequence is periodical from some point.

$N = 15$, $x = 7$ in $\mathbb{Z}_{15}$.

$\#\mathbb{Z}_{15}^\times = 8$

$1, 7, 4, -2, \dots$ Again: periodic! period 4

$N = 7$, $x = 2$ ...

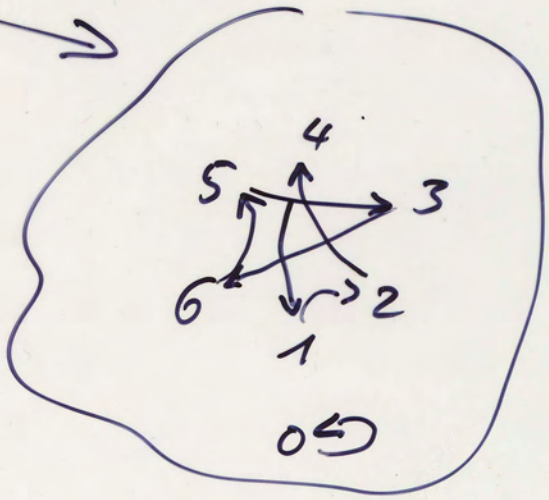
$\#\mathbb{Z}_7^\times = 6$

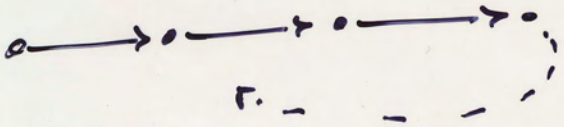
$1, 2, 4, \dots$ period 3

$N = 15$, $x = 3$

$1, 3, -6, -3, 6, \dots$

$\#\mathbb{Z}_{16}^\times = 8$ period 4

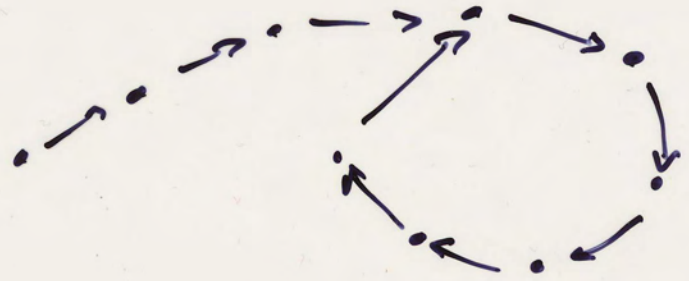




(i) The set of possible elements is finite.

(ii) The successor of an element is determined.

$\Rightarrow$ There must be repetition.



Observe

If x is invertible, so is any power x^k of it.

In other words: if $x \in \mathbb{Z}_N^\times$ so is any

$$x^k \in \mathbb{Z}_N^\times.$$

Thus the longest ~~possible~~ finitable repitition length is $\# \mathbb{Z}_N^\times$ in case $x \in \mathbb{Z}_N^\times$.

Now:

$$\# \mathbb{Z}_6^\times = \# \{1, -1\} = 2$$

$$\# \mathbb{Z}_{16}^\times = \# \{\pm 1, \pm 2, \pm 4, \pm 7\} = 8$$

$$\# \mathbb{Z}_7^\times = 7 - 1 = 6$$

Lemma If p is prime, then $\# \mathbb{Z}_p^\times = p - 1$.

Observation

The period in all our examples divides the number of invertible elements

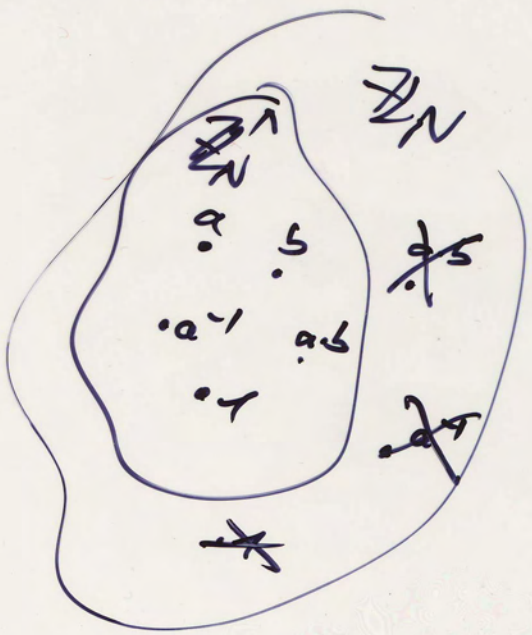
commutative
G group : a set G
an operation ·
such that axioms PANIC
hold.

Further: all our groups are finite.

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

P : Take $a, b \in \mathbb{Z}_N^\times$. Then $a \cdot b \in \mathbb{Z}_N^\times$.
A : $(ab)c = a(bc)$ trivially. $(a^{-1}b^{-1}) \cdot (ab) = a^{-1}a \cdot b^{-1}b = 1 \cdot 1 = 1$.
N : $1 \in \mathbb{Z}_N^\times$
I : Take $a \in \mathbb{Z}_N^\times$. Then $a^{-1} \in \mathbb{Z}_N^\times$ because $a \cdot (a^{-1}) = 1$.
C : ✓

(**Examples** $(\mathbb{Z}_N, +)$ is also a comm. group.)



Thm (Lagrange)

Suppose G is a finite group and $x \in G$ any element.
Then

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

In other words: $\#G$ is repetition length for the sequence $1, x, x^2, x^3, x^4, \ldots$

Pf We prove this only for ~~commutative~~ commutative groups.
Write down a list of all group elements:

$$g_1, g_2, \ldots, g_s$$

with $s = \#G$.
Multiply each list member by x:

$$xg_1, xg_2, \ldots, xg_s .$$

Claim This is also a list of all group elements.
(a) All new elements are pairwise distinct.
⌜ Suppose $xg_i = xg_j$. Multiply by x^{-1}.
Thus $\underset{g_i}{\underset{\shortparallel}{x^{-1}xg_i}} = \underset{g_j}{\underset{\shortparallel}{x^{-1}xg_j}}$, thus $i = j$. ✓ ⌟

(b) Any group element occurs on the new list.
⌜ Take any element of G, say g_i.
We look for j with $xg_j = g_i$. Equiv. $g_j = x^{-1}g_i$.
Since $x^{-1}g_i$ is a group element, it occurs on the first list, i.e. there is such a j.

⌟

So

$$g_1 \cdot \ldots \cdot g_s = xg_1 \cdot xg_2 \cdot \ldots \cdot xg_s$$

because the lists coincide up to order and the group is commutative.

Thus

$$\underbrace{g_1 \cdot \ldots \cdot g_s} = x^s \cdot g_1 \cdot \ldots \cdot g_s .$$

Multiply by $(g_1 \cdot \ldots \cdot g_s)^{-1}$:

$$1 = x^s .$$

That is what we wanted since $s = \#G$. □

Corollary (Euler)

Suppose $N > 2$ and $x \in \mathbb{Z}_N^\times$.

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

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

φ ← Euler totient function.

□

Corollary (Little Fermat Theorem)

Suppose p is prime and $x \in \mathbb{Z}_p^\times$.

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

Pf Apply Euler's theorem with $N = p$ and observe $\varphi(p) = p - 1$.

($\varphi(p) = \#\mathbb{Z}_p^\times$)

□

Corollary ~~Fermat's little theorem~~

Suppose p is prime and $x \in \mathbb{Z}_p$.

Then $$x^p = x \quad (\text{in } \mathbb{Z}_p).$$

Pf
- For $x \in \mathbb{Z}_p^\times$ this is clear.
- Otherwise $x = 0$ in $\mathbb{Z}_p$.
  Thus $x^p = 0^p = 0 = x$.

→ Both cases give the result. □

Why is RSA correct?

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

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

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

Now $ed = 1 + k \cdot L$ for some $k \in \mathbb{Z}$,

where $L = (p-1)(q-1)$.

Thus $z = x^{1 + k \cdot L} = x \cdot (x^L)^k$.

// **Fact** $\varphi(N) := \#\, \mathbb{Z}_N^\times = L$.

In case x is invertible we have $x^L = 1$.

and thus $z = x \cdot 1^k = x \cdot 1 = x$!

What about the fact that $\#\, \mathbb{Z}_{p \cdot q}^\times = (p-1)(q-1)$?

~~If~~ the $\gcd(x, p \cdot q)$ could be

1, p, q or $p \cdot q$,

and nothing else

~~0~~, 1, 2, 3, ... ~~p~~ ~~q~~ ~~2p~~ ~~3q~~ ~~q-1 p~~ , pq-1

q-1 elements have $\gcd(x, pq) = p$

p-1 $= q$

1 $\gcd(x, pq) = p \cdot q$

all other elements have $\gcd(x, pq) = 1$.

Thus there are $pq - q + 1 - p + 1 - 1$ invertible elements

$= (p-1)(q-1)$

So we have proved $\# \mathbb{Z}_{pq}^{\times} = (p-1)(q-1)$

ie. $\varphi(N) = L$

□

towards the Chinese Remainder Theorem

teacher puts papils in rows of 2
→ 1 pupil remains.

teacher puts pupils in rows of 3
→ 1 pupil remains.

teacher puts pupils in rows of 5
→ 3 remain.

How many pupils were there?

Rephrase that: Find the number x such that

$$x \equiv 1 \quad \text{modulo } 2,$$
$$x \equiv 1 \quad \text{modulo } 3,$$
$$x \equiv 3 \quad \text{modulo } 5.$$

The answer is $x = 13$ or $x = 43 = 13 + 2 \cdot 3 \cdot 5$
or $x = 73$ or ...

For short: $x \equiv 13$ modulo 30.

Chinese Remainder Theorem

Suppose $N = N_1 N_2$ with $\gcd(N_1, N_2) = 1$.

Then the map

$$\begin{aligned} \mathbb{Z}_N &\longrightarrow \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \\ x \bmod N &\longmapsto (x \bmod N_1,\ x \bmod N_2) \end{aligned}$$

is well-defd, structure preserving, injective (1-1), and surjective. In other words: it is an isomorphism

Example

$\mathbb{Z}_{15}$ elements mod 15 $\times$ $x+15$

$\mathbb{Z}_3$ elements mod 3

$\mathbb{Z}_5$ elts mod 5

CRT, down to earth version

Given $N = N_1 N_2$ with $\gcd(N_1, N_2) = 1$ and $a_1, a_2 \in \mathbb{Z}$. Then there exists an $x \in \mathbb{Z}$ with

$x \equiv a_1$ modulo N_1 and

$x \equiv a_2$ modulo N_2.

Example

Consider $N=15$, $x=7$ in $\mathbb{Z}_{15}$

We had the sequence

$\mathbb{Z}_{15}$: $1 \xrightarrow{\cdot 7} 7 \xrightarrow{\cdot 7} 4 \xrightarrow{\cdot 7} -2 \xrightarrow{\cdot 7} 1, \ldots$ → reduce

$\mathbb{Z}_3$:	1	1	1	1	1
×	1	2	-1	-2	1
$\mathbb{Z}_5$					

Let's rebuild the sequence in $\mathbb{Z}_3 \times \mathbb{Z}_5$

7 → reduce

$\mathbb{Z}_3$	1	1	1	1	1
×	1	2	-1	-2	1
$\mathbb{Z}_5$					

$\cdot(1,2)$ $\cdot(1,2)$

$\cdot(1,2)$ ← reduction of 7 : $(7 \bmod 3, 7 \bmod 5) \cong (1,2)$

So it is the same whether we think

in $\mathbb{Z}_{15}$, or

in $\mathbb{Z}_3 \times \mathbb{Z}_5$.

Example $N = 3 \cdot 7$, $x = 4$

$\mathbb{Z}_N$: $1 \xrightarrow{\cdot 4} 4 \xrightarrow{\cdot 4} -5 \xrightarrow{\cdot 4} 1, \ldots$

↓

$\mathbb{Z}_3$	1	1	1	1	…
×	1	-3	2	1	…
$\mathbb{Z}_7$					

$x \cong (4 \bmod 3, 4 \bmod 7) = (1, -3)$

$\cdot(1,-3)$ $\cdot(1,-3)$

1	1	1	1	…
1	-3	2	1	…

$\mathbb{Z}_6$:	0	1	2	3	4	5
112						
$\mathbb{Z}_2$:	0	1	0	1	0	1
× :	0	1	2	0	1	2
$\mathbb{Z}_3$						

$\mathbb{Z}_2 = \{0,1\}$

$\mathbb{Z}_3 = \{0,1,2\}$

↓ pairs

$(0,0), (0,1), (0,2),$
$(1,0), (1,1), (1,2)$

$$3 \underset{\mathbb{Z}_6}{+} 4 \;\hat{=}\; (1,0) + (0,1)$$
$$= (1+0, 0+1)$$
$$= (1,1) \;\hat{=}\; 1$$

Which are the invertible elements?

To compute the inverse of the map in the CRT, i.e. to find a solution x in the down-to-earth version you may use EEA.

$3^{100} \bmod 11$

3^{100} in $\mathbb{Z}_{1001}$ $\qquad 100 = 0110\ 0100_2$

$\varphi(7 \cdot 11 \cdot 13)$
$\|$
$6 \cdot 10 \cdot 12 = 720$

$3^{10} = 9$

$3^{11} = 27$

$3^{110} = 729$

$1001 = 0$
$1000 = -1$

$3^{1100} = 531\,441$

$= 531 \cdot \underbrace{1000}_{-1} + 441$

$= -531 + 441$

$= -90$ ⟸ 1

$3^{11000} = (90)^2$

$3^{11001} = \boxed{(90)^2} \cdot 3$

$27 \cdot 27$
54
189
$729 \cdot 729$
531 441

441
-531

---

division with remainder

$a, b \in \mathbb{Z}, b > 0$

$a = q \cdot b + r, \quad 0 \le r < b$ 1

What is a polynomial?
It is linear combination of powers of same variable(s).

Ex $\underbrace{5}_{\in \mathbb{Z}} \underbrace{x^2}_{\in \mathbb{Z}} + \underbrace{1}_{\in \mathbb{Z}} x - \underbrace{2}_{\in \mathbb{Z}}$ is a polynomial „over $\mathbb{Z}$".

$\underline{n}^3 + 2\underline{n} \in \mathcal{O}(\underline{n}^3)$

↑ degree = 3

Ex $\underbrace{5}_{\in \mathbb{Z}_{11}} x^2 + \underbrace{1}_{\in \mathbb{Z}_{11}} x - \underbrace{2}_{\in \mathbb{Z}_{11}}$ is a polynomial over $\mathbb{Z}_{11}$.

$$(5x^2 + x - 2)^2$$

$$= (5x^2 + x - 2) \cdot (5x^2 + x - 2)$$

$$= 5x^2(\quad) + x(\quad) - 2(\quad)$$

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

$$+ (5 \cdot (-2) + 1 \cdot 1 + (-2) \cdot 5)\, x^2$$

$$+ (1 \cdot (-2) + (-2) \cdot 1) x + (-2) \cdot (-2)$$

$$= 3x^4 + 1x^3 + 3x^2 - 4x + 4$$

$\mathbb{Z}_2 = \{0, 1\}$

$\mathbb{Z}_2[x] \ni \overbrace{x^3 + x + 1}^{a} = \overbrace{(x + 0)}^{q}\overbrace{(x^2 + 1)}^{b} + \overbrace{1}^{r}$

coeffs ↑ variable $\quad - (x^3 + x)$

$\quad 1$

quotient, remainder

division with remainder for polynomials over a field

$a, b \in \underbrace{F[x]}_{\text{field for coeffs.}}, b \neq 0$ the variable

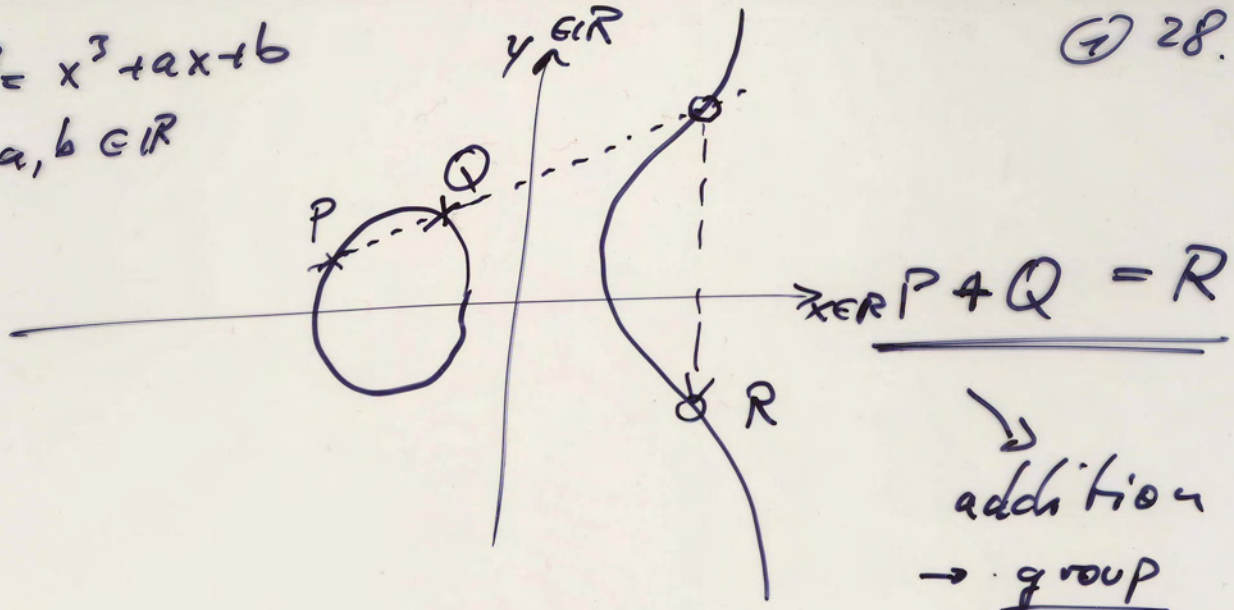
$a = q \cdot b + r, \quad (r = 0 \text{ or } \deg(r) < \deg(b))$

$\deg(0) := -\infty.$

largest exp. of x in r

$y^2 = x^3 + ax + b$

$a, b \in \mathbb{R}$



$P + Q = R$

→ addition

→ group

way to do this:

write P by coordinates

Q

find a formula for the coordinates of R.

$x_P^2 + \dots \; x_Q y_P \dots$

To get a finite group:

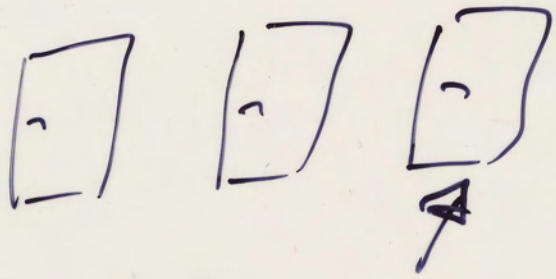
use coefficients/numbers but from $\mathbb{Z}_p$ for some prime p.

This formula depends highly on the representation of the points P, Q.

Probability

- error detection
- input distribution + reaction to it & randomized algorithms
- gambling : winning probability, expected win
  - ↳ coin tossing

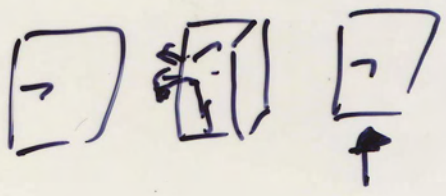
Monty Hall Problem



choose one

host opens another with goat.

do you switch?



Factoring

Pollard-ρ

Suppose you are given a number N.
You want to compute a factor p of N.

Solution proposed

Fix a function $f : \mathbb{Z}_N \to \mathbb{Z}_N$
and a seed $x_0 \in \mathbb{Z}_N$.

Compute x_0, $x_1 = f(x_0)$,
$x_2 = f(x_1)$,
$x_3 = f(x_2)$,
...

until two of them coincide modulo p!
We can detect that without knowing p by computing

$$p := \gcd(x_i - x_j, N) \neq 1$$

Heuristically: expected time $\sqrt{N}$

$\approx 2^{n/4}$ if $n = \#$ bits in N

Algo

Input: N.
Output: either a factor p or FAIL.

1. $x_0 \in_R \mathbb{Z}_N$ // $:=$ x_0 (Choose at random), $i := 0$
2. repeat
3. $i++, x_i = f(x_{i-1})$, $y_i = f(f(y_{i-1}))$, ...
4. until $g := \gcd(x_i - y_i, N) \neq 1$.
5. return g if $g \neq N$ or FAIL if $g = N$.

Consider a program with a loop

1. repeat
2. something
3. until condition holds.

where prob(condition holds) $= \frac{1}{42}$.

How many iterations of the loop do you expect?

More concrete

1. repeat
2. $n \in_R \mathbb{Z}_{42}$
3. until $n = 0$.

What is the average (=expected) running time?

42!

Send me an email to

nueske@b.it.uni-bonn.de

---

finite probability space

Ω finite set

$P: \Omega \to [0,1]$

such that $\sum_{u \in \Omega} P(u) = 1$

Example coin tossing: "fair coin"

$\Omega = \{ \text{heads}, \text{tails} \}$

$P(\text{heads}) = \frac{1}{2}, \quad P(\text{tails}) = \frac{1}{2}.$

coin tossing including "rim"

$\Omega = \{ \text{heads}, \text{rim}, \text{tails} \}$

$P(\text{heads}) = 0.499,$

$P(\text{tails}) = 0.499,$

$P(\text{rim}) = 0.002$

1 die
2 dice

rolling a three sided die

$\Omega = \{ \cdot, \cdot\cdot, \cdot\cdot\cdot \}$

$P(\cdot) = \frac{1}{3}, \quad P(\cdot\cdot) = \frac{1}{3}, \quad P(\cdot\cdot\cdot) = \frac{1}{3}$

rolling a "special" die

$\Omega = \{ \cdot, \cdot\cdot, \cdot\cdot\cdot \}$

$P(\cdot) = \frac{4}{6}, \quad P(\cdot\cdot) = \frac{1}{6}, \quad P(\cdot\cdot\cdot) = \frac{1}{6}$

Ex fair die

$\Omega = \{1, 2, 3, 4, 5, 6\}$

$P(i) = \frac{1}{6}$ for each $i \in \Omega$.

prob(roll an even number) =

$= P(2) + P(4) + P(6) = \frac{1}{2}$.

This is an example of a uniform distribution (P is called distribution)

An event is a subset of Ω, $A \subseteq \Omega$.

We define $\text{prob}(A) := \sum_{u \in A} P(u)$

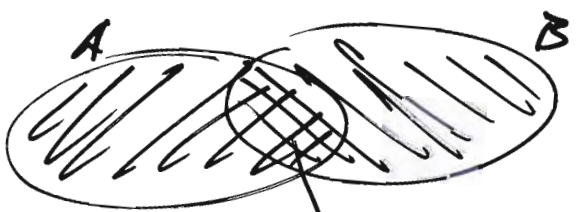
Now obviously we have:

- null event $\emptyset = \{\}$: $\text{prob}(\emptyset) = 0$
- Ω : $\text{prob}(\Omega) = 1$.
- Suppose $A, B \subseteq \Omega$, $A \cap B = \emptyset$.

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

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

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



$\dot{2}$ $prob(A \cap B) \overset{?}{=} prob(A) \cdot prob(B)$?

Ex fair die:

$A = \{2,4,6\}$, $B = \{4,5,6\}$.

$prob\ A = 1/2$

$prob\ B = 1/2$

$prob(A \cap B) = prob\{4,6\} = 1/3 \neq 1/2 \cdot 1/2$.

→ A and B are not independent.

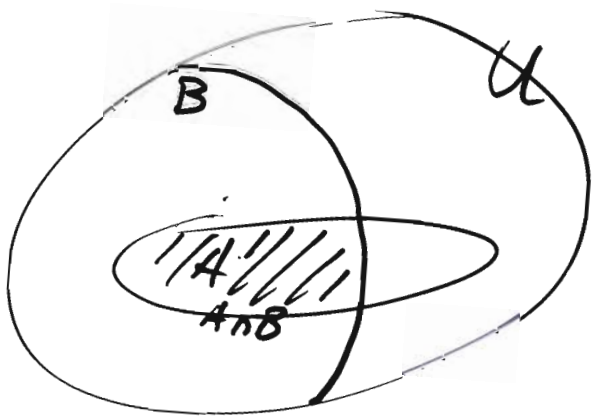
Define: two events A and B are called independent iff

$$prob(A \cap B) = prob(A) \cdot prob(B).$$

Suppose A, B are events, $probB \neq 0$.

conditional probality of A given B

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



We can read the cond. prob. $prob(\cdot \mid B)$ as having shrunk the universe to B and adapting the distribution:

$$(B, u \mapsto prob(\{u\} \mid B))$$

fair die

Ex $A = \{2, 4, 6\}$

$B = \{1, 2\}$ $\quad A \cap B = \{2\}$

$prob(A \mid B) = \frac{1}{2}$, $\quad \frac{prob(A \cap B)}{prob(B)} = \frac{1/6}{1/3} = \frac{1}{2}$.

Now A and B are independent

iff $prob(A \mid B) = prob(A)$

Ex Monty Hall example

$U = \{1, 2, 3\}$

$P(u) = \frac{1}{3}$ for any $u \in U$.

$B = \{1, 2\}$

$prob(1 \mid B) = \frac{prob(1)}{prob(B)} = \frac{1/3}{2/3} = \frac{1}{2}$.

$prob(2 \mid B) = \frac{1}{2}$.

This does <u>not</u> describe the <u>show</u>.

Right answer:

$prob(\text{car w/o switch}) = prob(\text{one door}) = \frac{1}{3}$

$prob(\text{car with switch}) = prob(\text{two doors}) = \frac{2}{3}$.

real random variable $X: \Omega \longrightarrow \mathbb{R}$ (3)

ω

This may also be sth. else

eg. X = running time of the program

1. repeat
2. $x \in_R \mathbb{Z}_{42}$
3. until $x = 0$.

expected value of X

$$E(X) = \sum_{u \in \Omega} X(u)\, P(u)$$

$$\overset{!}{=} \sum_{x \in X(\Omega)} x \cdot \text{prob}(\underbrace{X = x}_{\{u \mid X(u)=x\}})$$

$$\sum_{x \in X(\Omega)} \sum_{\substack{u \in \Omega \\ X(u)=x}} \underbrace{X(u)}_{x} P(u) = \sum_{x \in X(\Omega)} x \cdot \sum_{\substack{u \in \Omega \\ X(u)=x}} P(u)$$

$$\text{prob}(\underbrace{\{u \mid X(u)=x\}}_{=: X=x})$$

u	a	b	c	d	e
	1	1	2	3	3

Ex fair die, $X(u) = u$.

$$E(X) = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6}$$

$$= \frac{21}{6} = 3.5.$$

variance $\quad \text{var}(X) = E\left((X - E(X))^2\right)$

standard deviation $\quad \sigma(X) = \sqrt{\text{var}(X)}$

Suppose X, Y random variables
(over the same universe)

X, Y <u>independent</u> iff

$$prob(X=x, Y=y)$$
$$= prob(X=x) \cdot prob(Y=y)$$

for all possible x, y.

Again: $prob(X=x \mid Y=y) = prob(X=x)$
(provided $prob(Y=y) \neq 0$). ⌟

Consider a program of the form

```
repeat
  body
until X_i = 1
```

What the expected running time
if $prob(X_i = 1) = p$ for all iterations i
and the r.v. X_i are p.w. independent?

$$prob(X_i = 0) = 1 - p =: q.$$

We fix a certain maximum time n,
which we'll let tend to infinity
at the end.

Define $Y^{(n)}$ as a new r.v.

such that $Y^{(n)} = i$ if $X_1 = 0, X_2 = 0, \dots, X_{i-1} = 0$ and $X_i = 1$. $(i \le n)$

$Y^{(n)} = n+1$ if $X_1 = \dots = X_n = 0$

this is the running time of our loop, provided it terminates within the first n iterations.

Calculate

$$E(Y^{(n)}) = \sum_{i=1}^{n+1} i \cdot \underbrace{\text{prob}(Y^{(n)} = i)}$$

Now in case $i \le n$:

$$\text{prob}(Y^{(n)} = i) = \text{prob}(X_1 = 0, X_2 = 0, \dots, X_{i-1} = 0, X_i = 1)$$

$$= \text{prob}(X_1 = 0) \cdot \text{prob}(X_2 = 0) \cdot \dots \cdot \text{prob}(X_{i-1} = 0) \cdot \text{prob}(X_i = 1)$$

$$= \underbrace{\sigma \cdot \dots \cdot \sigma}_{i-1} \cdot \varrho = \sigma^{i-1} \varrho$$

and

$$\text{prob}(Y^{(n)} = n+1) = \sigma^n$$

Thus

$$E(Y^{(n)}) = \underbrace{\sum_{i=1}^{n} i \, \sigma^{i-1} \varrho} + (n+1)\sigma^n.$$

$$\sum_{i=0}^{n} \sigma^i = \frac{1 - \sigma^{n+1}}{1 - \sigma}$$

$$\sum_{i=0}^{n} i \sigma^{i-1} = \frac{n\sigma^{n+1} - (n+1)\sigma^n + 1}{(1-\sigma)^2}$$

We know $$\sum_{i=0}^{n} \sigma^i = \frac{1-\sigma^{n+1}}{1-\sigma}$$

$$(1-\sigma)\cdot\sum = 1+\sigma+\dots+\sigma^n - \sigma-\dots-\sigma^n-\sigma^{n+1}$$
$$= 1-\sigma^{n+1}. \quad \square$$

Derive this w.r.t. σ:

$$\sum_{i=0}^{n} i\,\sigma^{i-1} = \frac{(1-\sigma^{n+1})\cdot(-1) - (n+1)\sigma^n(1-\sigma)}{(1-\sigma)^2}$$

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

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

$$\overset{?}{=} \frac{-n\sigma^n}{1-\sigma} + \frac{1-\sigma^n}{(1-\sigma)^2}.$$

(Ex!)

Back to our calculation

$$E(Y^{(n)}) = \underbrace{\sum_{i=0}^{n} i\sigma^{i-1}}_{\frac{1}{(1-\sigma)^2}} \cdot\, p + (n+1)\sigma^n$$

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

$$= \frac{1-\sigma^n}{1-\sigma} + \sigma^n$$

$$= \frac{1}{p} + \underbrace{\sigma^n}_{<1}\left(1-\frac{1}{p}\right)$$

We let $n\to\infty$:

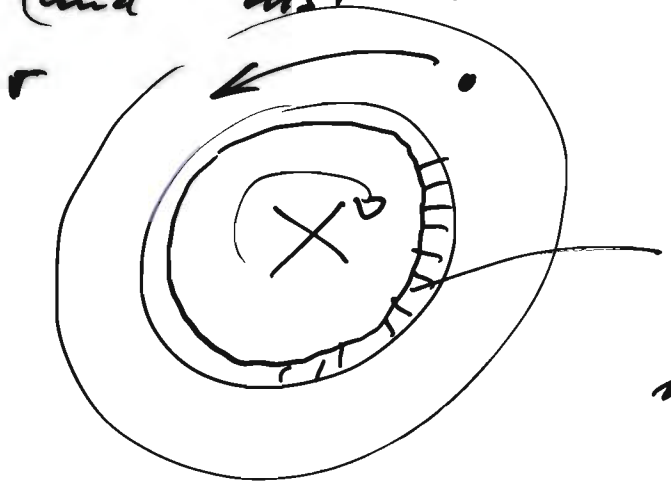
expected running time: $\lim_{n\to\infty} E(Y^{(n)}) = 1/p$. $\square$

Theorem

The expected running time of a loop which terminates independently after an iteration with probability $p > 0$ is equal to $1/p$.

due to Friday (17) 23.

Ex 2.1 (a) What is the appropriate probability space (and distribution) for Roulette?



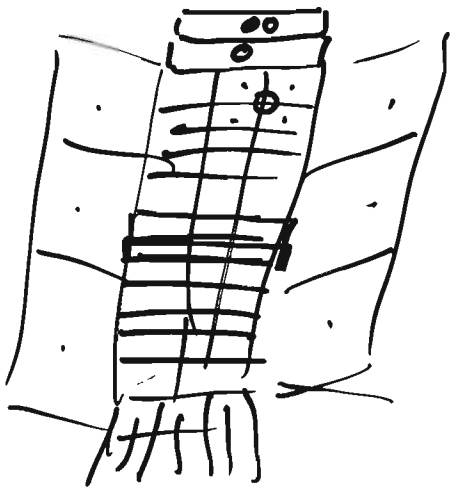
You can bet

(a) on a single number
payoff 36 x amount

(b) on halfs:
even / odd
high / low
red / black
} each of these 6 cases comprises 18 of the numbers 1...36
payoff 2x amount

(c) on thirds

(d) ....



Ex 2.1 (b) Compute the probability for "even", "high", the column of numbers divisible by 3 (not including 0, 00) for a quartett.

(c) Compute the expected pay off if you bet
(i) only on single numbers,
(ii) only on "halfs".

Ex 2.2 (a) Set up a prob. space for rolling 3 dice and a r.v. X_1, X_2, X_3 for each of the dice.

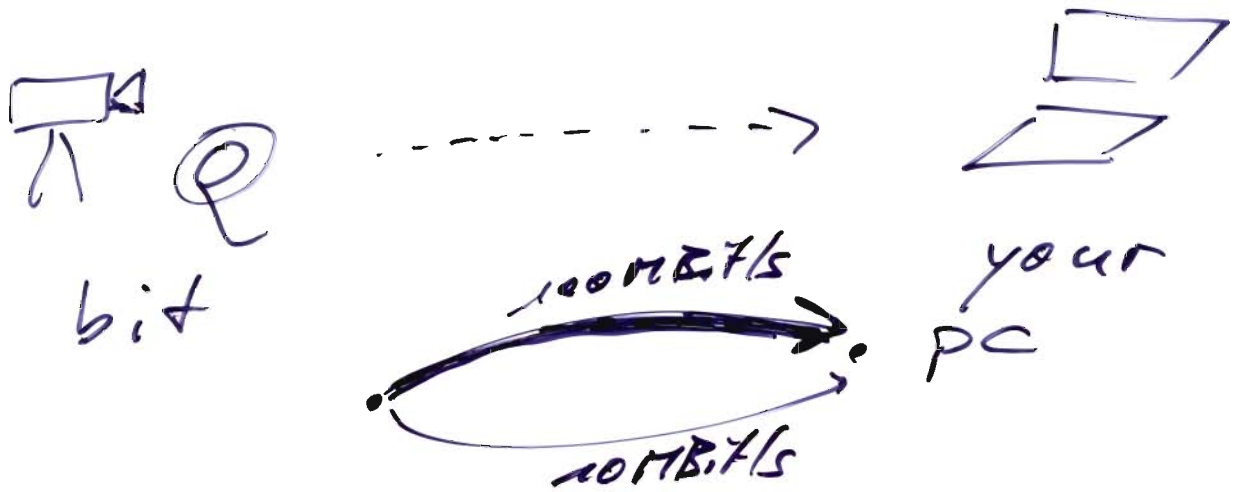
(b) What is the expected sum of the dice?

(c) Calculate the probability that
(i) all three dice show the same number,
(ii) all three dice show a different number.

(d) Calculate the cond. probability that the sum of the dice is even given none shows a six.

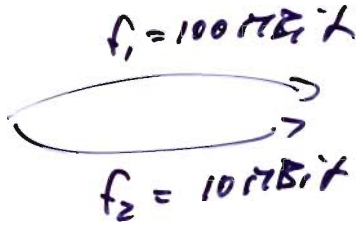
Ex 2.3 Give an new example where an average running time has to be computed and do so.

Streaming application

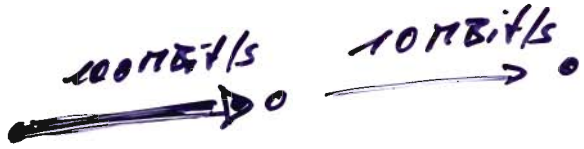


How to transmit?

f = 100 MBit



F = 1 sec



f = 100 MBit

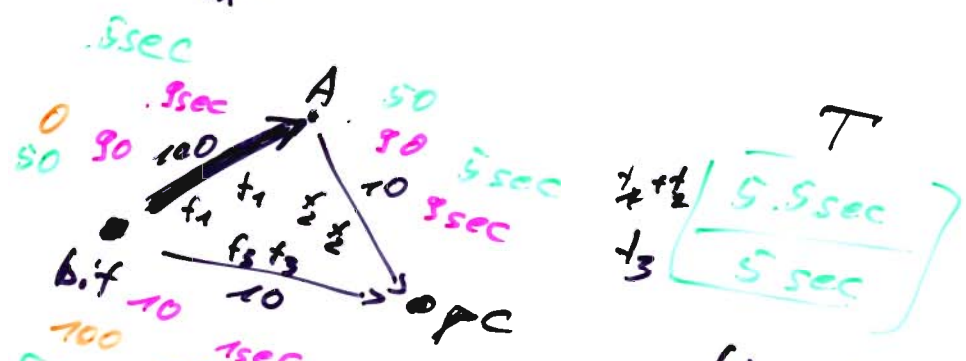
f_1 = 100 MBit

t_1 = 1 sec

f_2 = 100 MBit

t_2 = 10 sec

T = 1 sec



f = 100

constraint: same time for any part of data

(to avoid buffering!)

Conditions

path eq.

$$T = t_1 + t_2$$

$$T = t_3$$

$$f = \; ? \; \cdot T$$

edge eq.

(1) $f_1 = 100 \text{ MBit/sec} \cdot t_1$

(2) $f_2 = 10 \text{ MBit/sec} \cdot t_2$

(3) $f_3 = 10 \text{ MBit/sec} \cdot t_3$

from now on we drop units „MBit" and „sec"

node equ.

(A) $f_1 = f_2$

(bif) $f_1 + f_3 = f$

(PC) $f_2 + f_3 = f$

equations = 8

unknowns = { 8 including f, T
~~9~~ if we consider f given.

actually the equations (A), (bif) and (PC) are dependent, we can drop one of them w/o loosing information.

Using (1), (2) and (3) we get

(A') $100\, t_1 = 10\, t_2$

(bif') $100\, t_1 + 10\, t_3 = f$

(PC') $10\, t_2 + 10\, t_3 = f$

(α') $T = t_1 + t_2$

(β') $T = t_3$

Now we have essentially 4 eq.
and 4 var.

	t_1	t_2	t_3	T	
(A')	100	-10	0	0	0
(bif')	100	0	10	0	f
✓ (pc')	0	10	10	0	f
✓ (α')	1	1	0	-1	0
✓ (β')	0	0	1	-1	0

$-\frac{21f}{210}$

$+2\cdot\frac{11f}{210}$

Gauß elimination / Gauß-Jordan algorithm

Allowed elementary operations:

- exchange rows
- multiply a row by a invertible number
- subtract/add a multiple of a row from/to another row.

•	1	1	0	-1	0
	0	0	1	-1	0
	0	1	1	0	f/10
	10	0	1	0	f/10
-	10	-1	0	0	0
	1	1	0	-1	0
	0	0	1	-1	0
	0	-1	1	0	f/10
	0	-10	1	10	f/10
	0	-11	0	10	0

	1	0	-1	0
	0	-1	1	0
	0	0	1	-1
	0	-10	1	10
	0	-11	0	10
	1	0	-1	-1	- f/10
	0	1	-1	0	f/10
	0	0	1	-1	0
	0	0	11	10	11 f/10
	0	0	11	10	11 f/10

1	0	0	-2	-f/10
0	1	0	1	f/10
0	0	1	-1	0
0	0	0	21	11 f/10
0	0	0	21	11 f/10
1	0	0	0	+ f/210
0	1	0	0	10 f/210
0	0	1	0	11 f/210
0	0	0	1	11 f/210
0	0	0	0	0

this is the Gauß-Jordan-algorithm

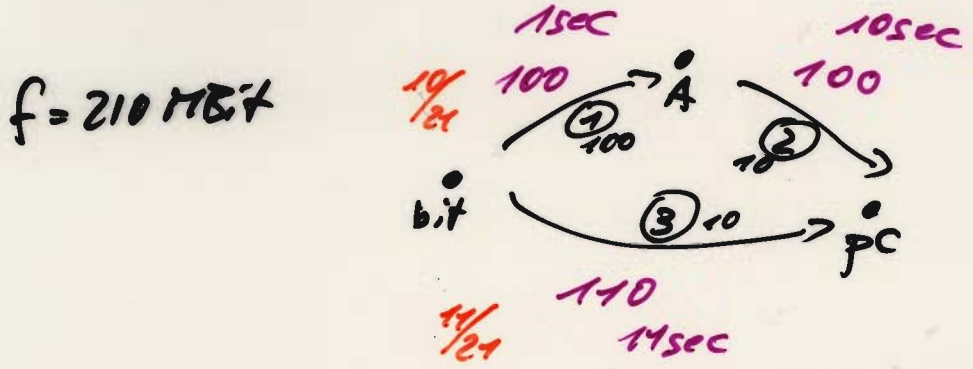
1e.

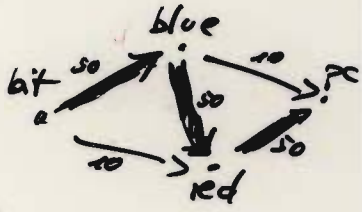
$t_1 = f/210$ $\quad f_1 = 100\ f/210$

$t_2 = 10\ f/210$ $\quad f_2 = 100\ f/210$

$t_3 = 11\ f/210$ $\quad f_3 = 110\ f/210$

$T = 11\ f/210$





Given: • a network incl. bandwidth
• a source and a dest.

Constraints

Putting data flows f_i and timings t_i

to each edge we get

- for each node the sum of the flows must equal zero (inflows are positive, outflows are negative).
- for each path from source to destination the sum of the timings must be equal to the total time T.
- for each edge $f_i = t_i \cdot$ bandwidth of the edge i

Matrices

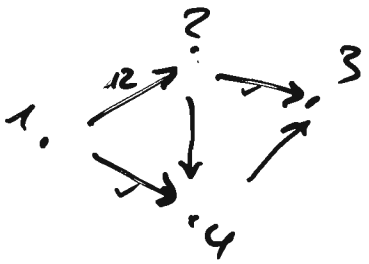
Ex adjecency matrices

Given a graph $G = (V, E)$ can be translated into a matrix A:

$A_{wv} = 1$ iff $\exists e \in E$: e is an edge from v to w.

(a_{wv})

Concrete graph:



$$A = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Matrix multiplication

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \text{not def.}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 10 & 3 \\ 3 & 22 & 9 \end{pmatrix}$$

$$\begin{array}{c|c} & \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 0 \end{pmatrix} \\ \hline \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \cdot \end{array}$$

$$C = A \cdot B$$

$$C_{wu} = \sum_{v} A_{wv} B_{vu}$$

Matrix multiplication can help us to count paths in graphs:

Paths of length are counted in A^2
(if A is the adjacency matrix)

because:

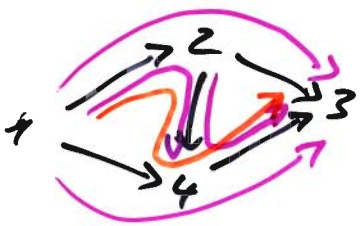
$$(A^2)_{wu} = \sum_v \underbrace{A_{wv}}_{\#\text{edges } w \to v} \underbrace{A_{vu}}_{\#\text{edges } u \to v}$$

$\#$ 2-paths $u \to v \to w$

$\#$ 2-paths $u \to w$

in the example

$$A^2 = \begin{array}{c} \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & & \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$



$1 \to 3$: 2
$1 \to 4$: 1
$2 \to 3$: 1

A^3 counts paths of length 3

here: $A^3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

$I + A + A^2 + \dots + A^{n-1}$ counts all paths of length $< n$.

Suppose G has no cycles: then $n = \#V$.

gives all the paths.

By computing $I + A + A^2 + \dots + A^{n-1}$
we can isolate the connected components.

If we replace addition with the or-operation,
then we still get the components.
(Instead of the # of paths an entry
just says whether there is a path or not.)

Side remark

Geometric sum:

$$I + A + \dots + A^{n-1} = (I - A^n)(I - A)^{-1}.$$

Pf.: $(I - A) \cdot (I + A + \dots + A^{n-1})$
$= I + A + \dots + A^{n-1}$
$\quad - A - \dots - A^{n-1} - A^n = I - A^n$. □

If the graph has no cycle
then $A^n = 0$ (when $n = \#V$)
thus $I + A + \dots + A^{n-1} = (I - A)^{-1}$

That might be a good way to
do the calculation.
(Actually it isn't!)

By the way: what is the cost of matrix
multiplication, say of $n \times n$-matrices?

$O(n^3)$ operations with entries $2.5n^2 - O(n)$
there cannot be an algo. with less than $2n^2 - 1$ op's

Do you think one can multiply matrices with $O(n^{2.9})$ op's?

or $O(n^{2.38})$ op's? Yes! ± 1980

Or $O(n^{2.37})$ op's? UNKNOWN

Yes! Strassen 1971

Gaussian elimination is not optimal.

Solving systems of linear equations

We know that we can express any such system in the form

$$A \cdot x = b$$

where A is a matrix and b is a vector and we want to know which vectors x solve this.

The elementary op's can be translated to matrix multiplication with "simple" matrices:

- exchange rows i, j

$$P_{ij} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & \cdots & 1 & \\ & & \vdots & \ddots & \vdots & \\ & & 1 & \cdots & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \quad \begin{matrix} & & i & & j \\ & & \downarrow & & \downarrow \end{matrix}$$

$$P_{ij} A x = P_{ij} b$$

- multiply a row i with an invertible number t

$$S_{i,t} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & t & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \quad \leftarrow i$$

$$S_{i,t} A x = S_{i,t} b$$

Als ersten Schritt zerlegen wir die Matrizen A, B und $C = A \cdot B$ in Blöcke der Größe $\frac{n}{2}$

$$\begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \cdot \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

n/2

Der entscheidende Schritt ist die Berechnung der folgenden Zwischenmatrizen:

$$W_1 = (A_{11} + A_{22}) \cdot (B_{11} + B_{22}), \quad W_2 = (A_{21} + A_{22}) \cdot B_{11}$$
$$W_3 = A_{11} \cdot (B_{12} + B_{22}), \quad W_4 = A_{22} \cdot (C_{11} + C_{21})$$
$$W_5 = (A_{11} + A_{12}) \cdot B_{22}, \quad W_6 = (A_{21} - A_{11}) \cdot (B_{11} + B_{12})$$
$$W_7 = (A_{12} - A_{22}) \cdot (B_{21} + B_{22}).$$

Die vier Blockmatrizen des Ergebnisses C sind

$$C_{11} = W_1 + W_4 - W_5 + W_2, \quad C_{12} = W_2 + W_4,$$
$$C_{21} = W_3 + W_5, \quad C_{22} = W_1 + W_3 - W_2 + W_6.$$

$T(n) \in 7\,T(\frac{n}{2}) + O(n^2)$

$T(n) \leq 7\,T(\frac{n}{2}) \; (+\; 18\,n^2), \quad T(1) = 1.$

Lets ignore additions:

$T(n) = 7\,T(\frac{n}{2}) \qquad T(1) = 1.$

Heuristics: $T(n) = 7\,T(\frac{n}{2}) = 7 \cdot 7 \cdot T(\frac{n}{4})$

$= 7 \cdot 7 \cdot 7 \cdot T(\frac{n}{8})$

Suppose $n = 2^k$ (i.e. $k = \log_2 n$) then $T(n) = 7^k \cdot \underbrace{T(\frac{n}{2^k})}_{1} = 7^k$

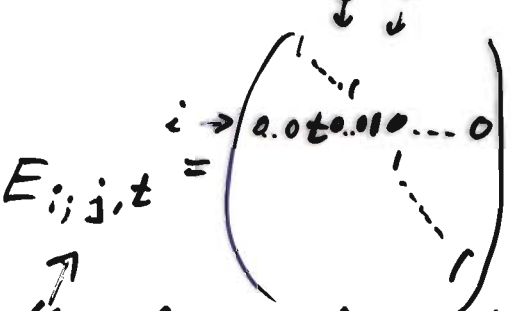
$\rightarrow T(n) = 7^{\log_2 n} = (2^{\log_2 7})^{\log_2 n}$

$= (2^{\log_2 n})^{\log_2 7} = n^{\log_2 7}$

$\log_2 7 \approx 2.80\ldots \leq 2.81$. thus $O(n^{2.81})$. is possible!

- add/subtract row j multiplied by t to/from row i

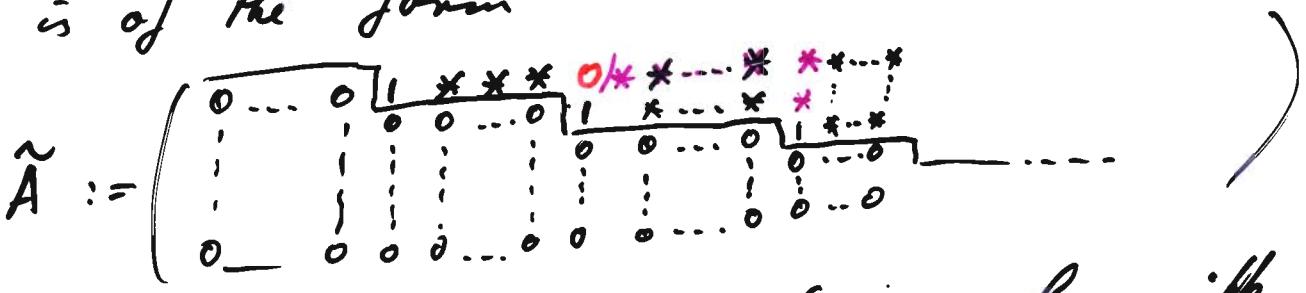
$$\underbrace{E_{i;j;t}\, A}\; x = E_{i;j;t}\, b$$

$E_{i;j,t} =$ 

either lower triangular

or upper triangular

Thm Suppose A is any matrix of format $m \times n$ and b is any vector of length n.
There is a sequence of elementary operations such that the resulting matrix is of the form

$\tilde{A} :=$ 

and this can be written as

$$\tilde{A} = F_r \cdots F_2 F_1 \cdot A$$

where each F_i is one of the elementary matrices and if we do not insist on $* = 0$ then each of them is lower triangular apart from the permutations (row swaps!) but these can be done in advance so we

$$\tilde{A} = \tilde{L} \cdot P \cdot A$$

where $\tilde{L}$ is lower triangular and P is a permutation.

Thm Being careful we obtain

$$P \cdot A = L \cdot U$$

where P is a permutation,
L is lower triangular
U is upper triangular
with only 0 and 1
on the diagonal. △

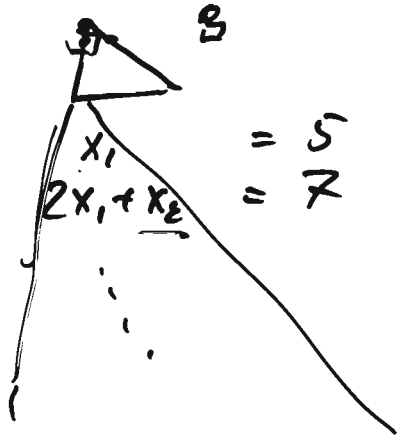
So to solve $Ax = b$

you can solve

$$PAx = Pb$$
$$\| $$
$$LUx$$

in two steps:

$$L\boxed{y} = Pb$$
$$\downarrow$$
$$Ux = y$$



Let's do this:

1.1
$$\left(\begin{array}{ccc|c|ccc} 1 & 6 & 8 & 4 & 1 & 0 & 0 \\ 3 & 5 & 13 & 0 & 0 & 1 & 0 \\ 12 & 2 & 10 & 1 & 0 & 0 & 1 \end{array}\right)$$

mod 13 over $\mathbb{Z}_{13}$

$$\left(\begin{array}{ccc|c|ccc} 1 & 6 & 8 & 4 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & -3 & 1 & 0 \\ 0 & -5 & 5 & 5 & 1 & 0 & 1 \end{array}\right)$$

1.5

$$\left(\begin{array}{ccc|c|ccc} 1 & 6 & 8 & 4 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 5 & 0 & 5 \\ 0 & 0 & 2 & 1 & -3 & 1 & 0 \end{array}\right)$$

$-5 \cdot 5 = 1$ by EEA

1.7

$$\left(\begin{array}{ccc|c|ccc} 1 & 6 & 8 & 4 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 5 & 0 & 5 \\ 0 & 0 & 1 & 1 & 7 & 7 & 0 \end{array}\right)$$

1 Gauß elimination

$2 \cdot 7 = 1$

DONE:

$\det = \frac{1}{1} \cdot \frac{1}{5} \cdot \frac{1}{7} \cdot (-1) \cdot U$

$L^{-1} \cdot P \cdot A$

$L^{-1} \cdot P$

$$L^{-1} = \begin{pmatrix} 1 & & \\ 5 & 5 & \\ -5 & 0 & 7 \end{pmatrix}$$

$$L = \begin{pmatrix} 1 & & \\ -5 & 7 & \\ +5 & 0 & 5 \end{pmatrix}$$

$$P^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \end{pmatrix} = P$$

Thus

$$\boxed{A = P^{-1} L U}$$

or

$$\boxed{PA = LU}$$

$\det A = -10 = -3.$ $\quad \det P = -1$ $\quad \det L = (\det L^{-1})^{-1} = (-1)^{-1} = -1$ (1 · 5 · 7) $\quad \det U = 1$

Questions

(i) How many solutions can there be? What kind of structure does the set of solutions have?

(ii) Is there some kind of formula that enables us to decide whether there are solutions or non zero solutions or unique solution? → Determinants.

Concerning (i):

To find all solutions of $Ax=b$ we have to find

- ~~find~~ one solution x_0 of $Ax=b$ ← the inhomogeneous equation

and

- all solutions δx of the homogenious equation $Ax=0$.

$A x_0 = b$, $A x_1 = b$ $\Rightarrow$ $A(x_0 - x_1) = 0$

What do you know about the set $S_A = \{ x \mid Ax = 0 \}$?

$0 \in S_A$, (λ a number, $x \in S_A \Rightarrow \lambda x \in S_A$), $x, y \in S_A \Rightarrow x+y \in S_A$. } S_A is a vector space over the coeff. field

over $\mathbb{Z}_{13}$

$$\left(\begin{array}{ccc|c} 1 & 6 & 8 & 4 \\ 1 & 0 & & -1 \\ & 0 & & 3/0 \end{array}\right) \Rightarrow$$

no solution because last line says:

$$0 \cdot x_3 = 3 \not\equiv 0.$$

$\Rightarrow$ dim 1 many solutions (over $\mathbb{Z}_{13}$: 13^1)

$$\left(\begin{array}{ccc|c} 1 & 6 & 8 & 4 \\ 1 & 0 & 1 & -1 \\ 0 & 0 & & 0 \\ 0 & & & 0 \end{array}\right) \Rightarrow$$

dim. 2 many solutions (over $\mathbb{Z}_{13}$: 13^2)

($\mathbb{Z}_{13} \times \mathbb{Z}_{13}$ $(0,0)$ $(0,1)$ ... $(0,12)$
$(1,0)$ $(1,1)$ ...
$\vdots$ $\vdots$
$(12,12)$)

Determinants

- $\det I = 1$
- $\det(A \cdot B) = \det A \cdot \det B$
- if P swaps rows
  $\det(PA) = -\det A$.
  $\det(AP) = -\det A$.
- $\det(S_{i,t} A) = t \cdot \det A$
- $\det(E_{i;jt} \cdot A) = \det A$

Fact

If A is an $n \times n$-matrix, b an n-vector then:

- $Ax = b$ is uniquely solvable iff $\det A \neq 0$.
- if $\det A = 0$ then $Ax = b$ is either unsolvable or it has several solutions

---

Ex 3.1 Solve the system of equations

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

and calculate the determinant of the matrix.

- → birthday problem ✓
- → Monty Hall
- → av. running time ✓
- → inverting polynomials modulo polynomials
- → example of solving a li. sys. + determinant

What do you want?

4 skip add. chain for 382

Birthday problem

$$\text{prob}\left(\begin{array}{l}\text{two birthdays coincide within } n \text{ randomly chosen persons}\end{array}\right)$$

$$= 1 - \underbrace{\text{prob}\left(\begin{array}{l}\text{within } n \text{ randomly chosen persons all have different birthdays}\end{array}\right)}_{=: p}$$

$$p = \frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdot \ldots \cdot \frac{(365-n+1)}{365}$$

$$= \left(1 - \frac{0}{365}\right)\left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right) \cdot \ldots \cdot \left(1 - \frac{n-1}{365}\right)$$

$$= 1 - \frac{\sum_{i=0}^{n-1} i}{365} + \frac{\text{small!}}{365^2}$$

$$1 - p = \frac{n(n-1)}{2 \cdot 365} - \frac{?}{365^2} \sim c \cdot n^2$$

Thus the expected number of persons until two have the same birthday will be about $c\sqrt{365}$. } No proof.

Actually, we consider the following

```
1 repeat
2     choose a person p_{i+1} with a random birthday
3 until (two of the persons p_1, ..., p_i
         have the same birthday)
```

Here, prob(Stopping after person i | all previous $i-1$ persons have diff. birthdays) $= \frac{i-1}{365}$.

Y = r. v. giving the number of persons until two have same birthd.

X_i = birthday of person i, $1 \le i \le \underline{366}$.

for $n \le 366$

thus $Y = n$ iff $X_n \in \{X_1, \dots, X_{n-1}\}$

& $\#\{X_1, \dots, X_{n-1}\} = n-1$

i.e. $X_1, \dots X_{n-1}$ are pairwise different.

Of course:

$$\text{prob}(X_i = x) = \frac{1}{365},$$

(x: same day in the year)

the r.v. $X_1, \dots, X_{366}$ are (~~pairwise~~) independent.

} hypotheses (= modeling the situation)

We want to calculate (or estimate) the expected running time.

$$E(Y)$$

So

$$E(Y) = \sum_{n=1}^{366} n \cdot \text{prob}(Y = n).$$

Now

$$\text{prob}(Y=n) = \text{prob}\Big(\boxed{X_n \in \{X_1, \dots, X_{n-1}\}} \;\&\; \boxed{X_1, \dots, X_{n-1} \text{ p.w. diff.}} \Big)$$

⚠ 1 ⚠ and are not independent!

Ex $n = 3$: is true, then

$$\text{prob}(\;|\;) = \frac{2}{365}$$

but if is false then

$$\text{prob}(\;|\; \neg \;) = \frac{1}{365}.$$

So depends on !

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

and thus rewriting gives

$$\text{prob}(A \cap B) = \text{prob}(A \mid B) \cdot \text{prob}(B).$$

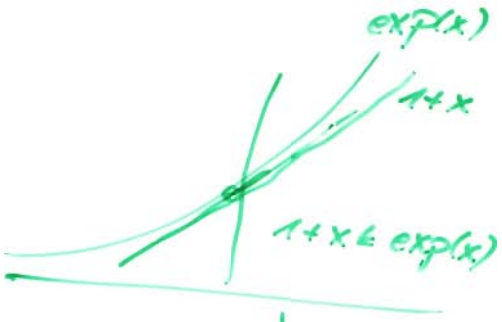
$$\text{prob}(Y=n) = \text{prob}(\square \mid \square) \cdot \text{prob}(\square)$$

We know

$$\text{prob}(\square \mid \square) = \frac{n-1}{365}$$

and

$$\text{prob}(\square) = \left(1-\frac{0}{365}\right)\left(1-\frac{1}{365}\right)\cdots\left(1-\frac{n-2}{365}\right) = \prod_{i=1}^{n-2}\left(1-\frac{i}{365}\right)$$



so putting this together yields

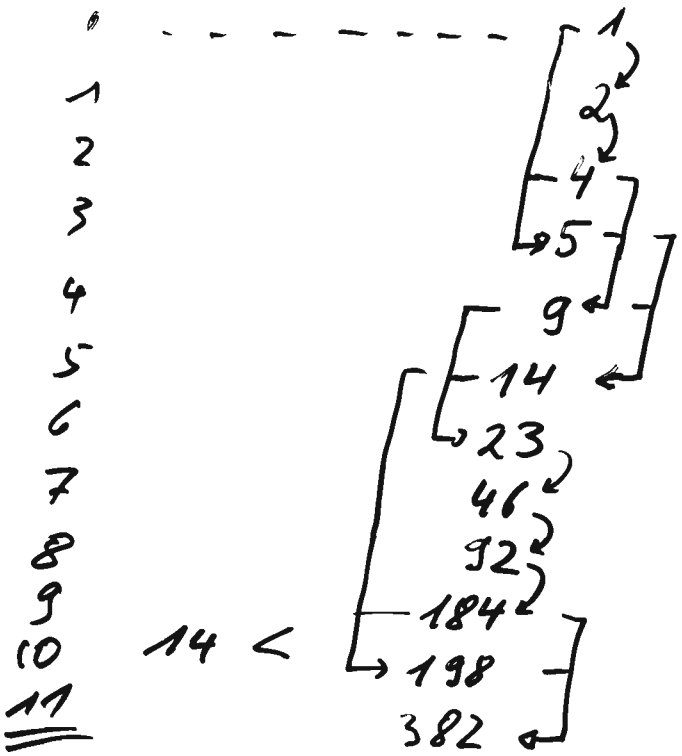
$$E(Y) = \sum_{n=1}^{366} n \cdot \frac{n-1}{365} \prod_{i=1}^{n-2}\left(1-\frac{i}{365}\right)$$

$$\left(1-\frac{i}{365}\right) \leq \exp\left(-\frac{i}{365}\right)$$

Now a "little maths manipulations" give

$$E(Y) \leq c \cdot \sqrt{365}.$$

11-element addition chain for $382 = 10111110_2$.



More info on that:

D.E. Knuth
The art of computer programming

---

in $\mathbb{Z}_7$ $\quad \frac{3}{2} = 3 \cdot 4 = \underline{\underline{-2}} = \underline{\underline{5}}$

in calculations only $-6, \ldots 6$,
(better: $-3 \ldots 3$ or $0 \ldots 6$).

$$-2 = 5$$

$$2^{-1} = 4 = -3 \text{ in } \mathbb{Z}_7.$$

Inverting polynomials in $\mathbb{Z}_2[x]$ 30.

$$\underbrace{(x^3+x+1)}_{\text{!!}\ A}{}^{-1} \text{ modulo } \underbrace{x^7+x^2+1}_{\text{!!}\ M}.$$

we look for a polynomial B such that

$$(B \cdot A) \text{ rem } M = 1$$

ie.

$$B \cdot A + K \cdot M = 1$$

for some polynomial K.

EEA

	r_i	q_i	s_i	t_i	
0	x^7+x^2+1		0	1	$0 \cdot A + 1 \cdot M = M$
1	x^3+x+1	x^4+x^2+x+1	1	0	$1 \cdot A + 0 \cdot M = A$
2	x^2	x	x^4+x^2+x+1	1	
3	$x+1$	$x+1$	$x^6+x^3+x^2+x+1$	x	
4	1	$x+1$	$x^6+x^5+x^2+x$ / x^7+x^2+1	x^2+x+1 / x^3+x+1	→ verified!
5	0				

Result: $1 = (x^6+x^5+x^2+x) \cdot A + (x^2+x+1) \cdot M$

Thus $A^{-1} \bmod M = x^6+x^5+x^2+x$.

div. w. rem.

$$\boxed{x^7+x^2+1} = (x^3+x+1)(x^4+x^2+x+1) + x^2$$

$$-(x^7+x^5+x^4)$$

$$x^5+x^4+x^2+1$$

$$-(x^5+x^3+x^2)$$

$$x^4+x^3+1$$

$$-(x^4+x^2+x)$$

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

$$\ldots$$

$$x^2$$

quotient; remainder

Solving linear equations

Let's calculate over $\mathbb{Z}_{19}$.

Problem

$$A = \begin{pmatrix} -3 & -7 & 1 \\ 2 & 4 & 3 \\ 0 & 7 & 8 \end{pmatrix}$$

Compute A^{-1} and $\det A$.
if it exists.

(Nice counting question:
How many invertible 3×3-matrices
are there over $\mathbb{Z}_{19}$?)

To find a matrix X
such $A \cdot X = I$.

(In other words: find x_1, x_2, x_3 vectors
such that $Ax_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $Ax_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $Ax_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}$.)

Gauß-Jordan

	-3	-7	1	1	0	0
	2	4	3	0	1	0
	0	7	8	0	0	1
	1	$-\frac{7}{3}$	6	6	0	0
$-2\,(\cdot)$	2	4	3	0	1	0
	0	7	8	0	0	1
	1	-4	6	6	0	0
$1:(-7)\,/\cdot 8$	0	-7	-3	7	1	0
	0	7	8	0	0	1
	1	0	5	2	-6	0
	0	1	-5	-1	8	0
$1:5\,/\cdot 4$	0	0	5	7	1	1
	1	0	0	-5	-7	-1
	0	1	0	6	9	1
	0	0	1	9	4	4

DONE.

$\mathbb{Z}_{13}$	
1	1
2	-9
3	-6
4	5
5	4
6	-3
7	-8
8	-7
9	-2

cubic! fine!

So: A is invertible,

and $A^{-1} = \begin{pmatrix} -5 & -7 & -1 \\ 6 & 9 & 1 \\ 9 & 4 & 4 \end{pmatrix}$

and $\det A = (-3)\cdot(-7)\cdot 5\cdot(-1)^0$ (no swaps.)

$= -9 \neq 0$

Other way for determinant:

Suppose $P \cdot A = L \cdot U$

(L: lower triang. △, U: upper triang. ▽)

then $\det A = \det L \cdot \det U$

$\det$ △ = $\prod$ diagonal elements

similar for $\det$ ▽ = ...