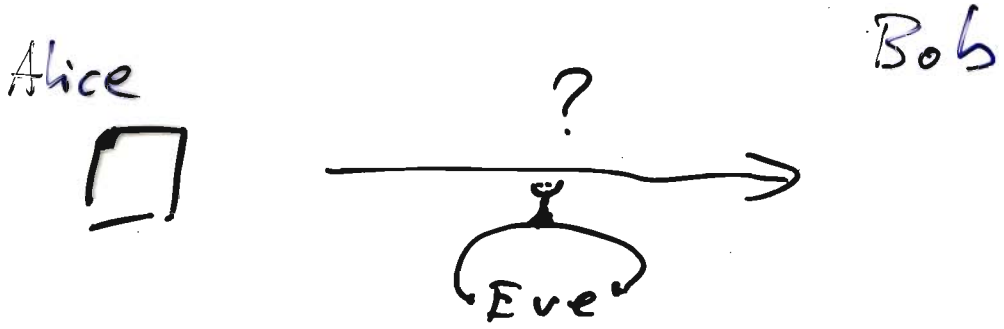
Task



How to?

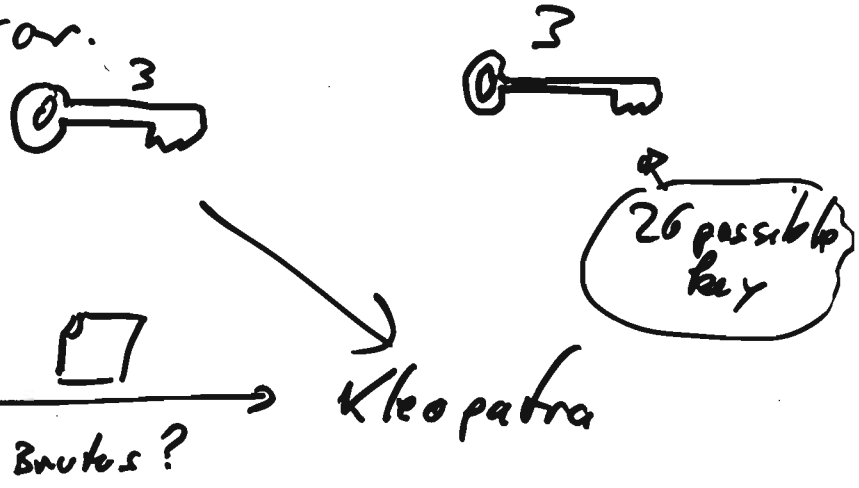
- Encrypt
  - → need key
  - → based on preshared knowledge like a codebook
    BUT WHEN YOU TRANSMIT this Eve learns it! ☹.

78: public key encryption??
?

classical: simplest:

Caesar cipher

replace any letter by its third successor.



What can Eve do?

→ frequency analysis

e.g. I find that H is most frequent
this indicates that an E is encrypted as an H (assuming that text was in English)

What else does Eve knows?
The encryption method
(because it's the worst case!)

<u>KERCKHOFFS' principle</u> (≈ 19th century)

[The attacker knows everything but the key.

In the example H is the third succ. of E. → hypothesis: key = 3.

→ try all keys. (Brute force attack)
Our example only has 26 keys. ☹

Better ciphers?

- Permutation cipher

A	B	C	D	E	.	.	L		U
↓	↓	↓							
F	X	A	D	Q			Y		B

BLUE $\xrightarrow{enc}$ XYBQ

keys = 26!

→ Brute force is now difficult
→ Frequency analysis breaks it!

23.10.06

(3)

- Vigenère cipher

key word: APPLE, A=0, P=16, P=16, L=11, E=4

QUEEN MARY TWO INCOMING TOMORROW.

APPLE APPL E APPLEAPPLE APPLEAPP

QKT .....

Addition mod 26

if we code A=0, B=1, ..., Z=25

A	B	C	D	E	F	...																		X	Y	Z
B	C	D	E	F	G	...																		Y	Z	A
C	D	E	F	G	H	...																		Z	A	B
D	E	F	G	H	I	...																		A	B	C
⋮																										
Z	A	_																								Y

Can Eve read a message without having the key?

~~Yes~~ the class says NO.

But: YES!

→ Brute force: $\#keys = 26 + 26^2 + 26^3 + 26^4 + \dots + 26^{10} + \dots + \underbrace{26^{20}}_{\text{practical ad-hoc limit.}}$

Computer nowadays can perform $\approx 10^{15}$ op's per day.

$\approx 2^{50}$ op's per day

So: $2^{60} - 2^{70}$ op's are feasible!

Computers can thus not try out all 20 letter words!

→ Finding key word length first and then attacking the remaining Caesar ciphers is possible & fast & with high probability!

<u>NOTE</u> If a cipher can be broken with non negligible (≡ not too small) probability, then already we call it <u>broken</u>.

- One-time Pad

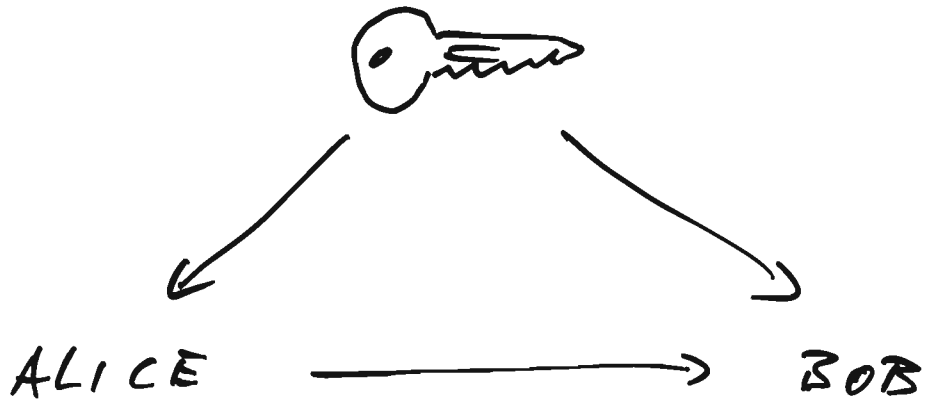
this is like Vigenère but
→ key length ≡ message length
→ key is completely random.

THIS cipher is
- provably (mathematically)
- absolutely secure

And it's more a less the only such one!

BUT: key length is HUGE!

Still situation:



Still the same picture!

[1971-74] British secret service: non-secret encryption]

1976 Diffie-Hellman found a way to agree on a key without prior information

1978 Rivest, Shamir, Adleman found RSA:

Choose key: Choose two prime numbers p, q of say 512-bits each.

$N := p \cdot q$.

$L := (p-1)\cdot(q-1)$ „repetition length"

Choose $d, e \in_R \{0, 1, \dots, L-1\}$ randomly such that L divides $de-1$,

i.e. $d \cdot e \equiv_L 1$ modulo L.

Public key (N, e).
Secret key (N, d).

Encrypt x: $y := x^e \underline{\text{rem}}\, N$. (modulo Operator)

Decrypt y: $z := y^d \text{ rem } N$

Hope: $z = x$!

A class: Integers modulo N, $\mathbb{Z}_N$

Parameter: a number $N \in \mathbb{N}$, $N \geq 2$.

Objects: integers in the range $0 \ldots N-1$.

Operations:

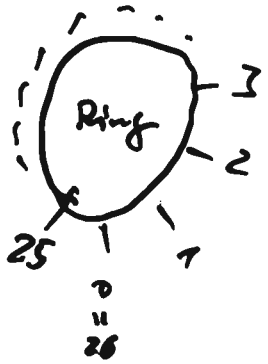
$$+ : (a,b) \longmapsto (a+b) \text{ rem } N.$$

$$\cdot : (a,b) \longmapsto (a \cdot b) \text{ rem } N.$$

$$- : a \longmapsto -a \text{ rem } N = \begin{cases} N-a & \text{if } a \neq 0 \\ 0 \end{cases}$$

$$1 : () \longmapsto 1,$$

$$0 : () \longmapsto 0.$$



Axioms:

Ring

- $P_+, P_\cdot$: operations must be properly defined
- $A_+, A_\cdot$: $\forall$ $(a+b)+c = a+(b+c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $N_+, N_\cdot$: $\forall$ $a+0 = a = 0+a$, $\forall$ $a \cdot 1 = a = 1 \cdot a$
- I_+ : $\forall a \; \exists b$: $a+b = 0 = b+a$, $a+(-a) = 0 = (-a)+a$
- $C_+, C_\cdot$: $\forall$ $a+b = b+a$, $a \cdot b = b \cdot a$
- D : $(a+b) \cdot c = ac + bc$, $a \cdot (b+c) = ab + ac$
- $0 \neq 1$.

Further rules (theorems):

Thm $\forall \quad a\cdot 0 = 0.$

Pf we have: $0+0 \overset{N+}{=} 0.$

Thus:
$$\begin{array}{ccc} a\cdot(0+0) & = & a\cdot 0 \\ \| D & & \\ a\cdot 0 + a\cdot 0 & & \end{array}$$

Add $-a\cdot 0$ to both sides:

$$\begin{array}{ccc} (a\cdot 0 + a\cdot 0) + (-a\cdot 0) & = & a\cdot 0 + (-a\cdot 0) \\ \| A+ & & \| I+ \\ a\cdot 0 + (a\cdot 0 + (-a\cdot 0)) & & 0 \\ \| I+ & & \\ a\cdot 0 + 0 & & \\ \| N+ & & \\ a\cdot 0 & & \end{array}$$

wwwwww

□

2nd Pf we have $a\cdot 1 \overset{N\cdot}{=} a$

Using $N+$ we have
$$\begin{array}{ccc} a\cdot(1+0) & = & a \\ \| D+ & & \\ a\cdot 1 + a\cdot 0 & & \\ \| N\cdot & & \\ a + a\cdot 0 & & \end{array}$$

Add $-a$ to both sides:
$$\begin{array}{ccc} (-a) + (a + a\cdot 0) & = & (-a) + a \\ \| A+ & & \| I+ \\ ((-a)+a) + a\cdot 0 & & 0 \\ \| I+ & & \\ 0 + a\cdot 0 & & \\ \| N+ & & \\ a\cdot 0 & & \end{array}$$

qed □

~~Ex~~ Example $\quad 4\cdot 5 = 6 \quad$ in $\mathbb{Z}_7$

Why is $I\cdot$ missing?

$I\cdot$: $\forall a\ \exists b:\quad a\cdot b = 1 = b\cdot a$

First: say $a=0$ then we ask for a b such that $(0\cdot b =)\ \underline{1}\ \{= b\cdot 0\}$

But as we just proved that

$$b\cdot 0 = \underline{0}$$

thus that would mean $1=0$.
This contradicts $0\neq 1$, and thus there is no such b.

But what about

$\overset{?}{\Rightarrow}$ $I\cdot'$: $\forall a\neq 0\ \exists b:\quad a\cdot b = 1 = b\cdot a$.

Note: this may be true eg. $a=2$ in $\mathbb{Z}_5$
Now: $2\cdot 3 = 1$. So have $\frac{1}{2} = 3$ in $\mathbb{Z}_5$.

Is $I\cdot'$ always true?

Let's check $\mathbb{Z}_5$:

$1\cdot 1 = 1$: 1 has inverse ✓
$2\cdot 3 = 1$: 2 has inverse ✓
$3\cdot 2 = 1$: 3 has inverse
$4\cdot 4 = 1$: 4 has inverse.

So in $\mathbb{Z}_5$ $I\cdot'$ is true! $\mathbb{Z}_5$ is a <u>FIELD</u>.

Next example: $\mathbb{Z}_6$.

$1 \cdot 1 = 1$ so 1 has inverse.

$\exists b$: $2 \cdot b = 1$

<u>1. Pf</u> Brute force:

$$\left.\begin{array}{l} 2\cdot 0 = 0 \\ 2\cdot 1 = 2 \\ 2\cdot 2 = 4 \\ 2\cdot 3 = 0 \\ 2\cdot 4 = 2 \\ 2\cdot 5 = 4 \end{array}\right\} \text{no } 1!$$

$\square$

<u>2nd Pf</u> 2 is even and 6 is even.
The equation $\{\boxed{2b = 1 \text{ in } \mathbb{Z}_6}\}$
means

$$\boxed{\begin{cases} 2b + 6\cdot k = 1 & \text{in } \mathbb{Z} \\ \text{for some } k. \end{cases}}$$

Observe that the left hand side is an integer combination of 2 and 6. And since both 2 and 6 are even, so is the left hand side $2b + 6k$. But 1 is not even. Thus the equation cannot be solved! $\square$

In $\mathbb{Z}_6$ I.' does <u>not</u> hold.

Ie. $\mathbb{Z}_6$ is <u>not</u> a field.

23.10.06

10

When does $\cdot^{-1}$ hold?

How can we obtain inverses and decide whether they exist?

Question: Given $x \in \mathbb{Z}_N$

Find $y \in \mathbb{Z}_N$ s.t. $\boxed{y x = 1 \text{ in } \mathbb{Z}_N}$.

As before we can translate this to a question about integers:

Given $x \in \mathbb{Z}$, $0 \le x < N$,

find $y \in \mathbb{Z}$ such that

$$\boxed{y \cdot x + k \cdot N = \boxed{1}^{\text{in } \mathbb{Z}} \text{ for some } k \in \mathbb{Z}.}$$

Example: $x = 7$, $N = 61$

Extended Euclidean Algorithm

	$y \cdot 7 + k \cdot 61$	q	y	k
(1) :	61		0	1
← (2) :	7	8	1	0
(1) − (2) :	[~~54~~]		[~~−1~~]	[~~1~~]
(1) − 2(2) :	[~~47~~]		[~~−2~~]	[~~1~~]
(1) − 8(2) :	5	1	−8	1
	2	2	9	−1
	1	2	−26	3
	0		61	−7

remainders

Division with remainders:

$61 = 8 \cdot 7 + 5$

$0 \le 5 < 7$

quotient

remainder

Last line says: $0 = 61 \cdot 7 + (-7) \cdot 61$

one but last line says:

$$(*) \qquad 1 = (-26)\cdot 7 + 3\cdot 61$$

We wanted to know the inverse of 7 in $\mathbb{Z}_{61}$.
Now $(*)$ means in $\mathbb{Z}_{61}$:

$$1 = (-26)\cdot 7 \boxed{\cancel{+\,3\cdot 0}} \text{ in } \mathbb{Z}_{61}$$

so

$$1 = 35 \cdot 7 \quad \text{in } \mathbb{Z}_{61}$$

ie.

$$\frac{1}{7} = 35 \quad \text{in } \mathbb{Z}_{61}.$$

An „unsuccessful" example:
$x=2, \quad N=6.$

$y\cdot 2 + k\cdot 6$		y	k
6		0	1
2	3	1	0
$\boxed{0}$ stop		-3	1

So last line reads: $0 = -3\cdot 2 + 1\cdot 6$

The one but last line says:

$$2 = 1\cdot 2 + 0\cdot 6$$

Division with remainder in $\mathbb{Z}$

Given two numbers $a, b \in \mathbb{Z}$, $b \neq 0$
find $q, r \in \mathbb{Z}$ such that

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

and

$$0 \leq r < |b|$$

<u>Thm</u> Such q, r always exist! $\triangle$

... prove this by induction...

<u>Thm</u> (EEA)

(a) If the EEA finds a solution to $\boxed{yx + kN = 1}$ then we have $\boxed{x^{-1} = y}$ in $\boxed{\mathbb{Z}_N}$, in particular: the inverse exists!

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

	r	q	$s^{(17)}$	$t^{(5)}$
$N \to$	17		1	0
$x \to$	5	3	0	1
	2	2	1	-3
$g \to$	$\boxed{1}$	2	-2	7
$0 \to$	0		5	-17

Check ✓

$$\boxed{1 = (-2)\cdot 17 + 7\cdot 5}$$ in $\mathbb{Z}$

↳ in $\mathbb{Z}_{17}$:

$1 = 7\cdot 5$

↳ $\frac{1}{5} = 7$ in $\mathbb{Z}_{17}$.

<u>Thm</u> The EEA computes

(i) the greatest common divisor g of the input elements N and x, as the last non-zero remainder.

(ii) integers s and t such that

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

So either $\underline{g=1}$ (or $g=-1$)

and $1 = sx + tN$

and $1 = sx$ in $\mathbb{Z}_N$

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

or $\underline{g \neq \pm 1}$ and $g \mid x$ and $g \mid N$

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

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

Sketch

$17 = 3 \cdot 5 + 2$

17	3	...
5		...
2		

Claim: $\gcd(17,5) = \gcd(5,2)$

In general:

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

$d \longrightarrow$

$\Longleftarrow d$

r_{i-1}	q_i	...
r_i		...
r_{i+1}		...

Proof that if $d \mid r_{i-1}$ and $d \mid r_i$ then $d \mid r_i$ and $d \mid r_{i+1}$

But that's trivial:

$$r_{i+1} = \underbrace{\underbrace{r_{i-1}}_{= d \cdot \bar{r}_{i-1}} - q_i \underbrace{r_i}_{= d \cdot \bar{r}_i}}_{d\,(\bar{r}_{i-1} - q_i \bar{r}_i)}$$

At the end we reach $\gcd(g,0) = g$

And vice versa!

Further obviously we have a loop invariant

$$r_i = s_i \cdot \overset{x}{\cancel{a}} + t_i \cdot \overset{N}{\cancel{b}}$$

$\triangle$

Def unit group of $\mathbb{Z}_N$:

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

$yx + kN = 1$ (in $\mathbb{Z}$)

Corollary

$$\mathbb{Z}_N^\times = \cancel{\{x \in \mathbb{Z}_N}$$

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

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

(ignoring type changes)

$x \in \mathbb{Z}_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
$\gcd(x,12)$	12	1	2	3	4	1	6	1	4	3	2	1

$$\hookrightarrow \mathbb{Z}_{12}^\times = \{ 1, 5, 7, 11 \}$$

$$= \{ \pm 1, \pm 5 \}$$

For RSA we now solved the problem how to find $d, e \in \mathbb{Z}_L$ such that $de = 1$ in $\mathbb{Z}_L$.

Namely: Repeat

Choose $d \in_R \mathbb{Z}_L$ (odd) at random.

Compute $g = \gcd(d, L)$ along with a representation $g = e \cdot d + k \cdot L$

Until $g = \pm 1$.

then $de = 1$ in $\mathbb{Z}_L$.

Corollary

$\mathbb{Z}_N$ is a field

$\iff \mathbb{Z}_N^\times = \mathbb{Z}_N \setminus \{0\}$

$\overset{!}{\iff}$ N is prime

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

If N is prime then is true

unless x is a multiple of N,

which happens only for $x = 0$

among the x with $0 \le x < N$.

If $\mathbb{Z}_N^\times = \mathbb{Z}_N \setminus \{0\}$, then N must be prime.

Otherwise, $N = a \cdot b$ for some $a, b \neq \pm 1$.

and then $\gcd(a, N) = a \neq 1$,

so $a \notin \mathbb{Z}_N^\times$ ↯. $\square$

Costs

Multiplication of two n-bit numbers:

$O(n^2)$ $\quad$ $O(n \log n \log\log n)$

EEA of two n-bit numbers

~~$O(n^3)$~~ $\quad$ $O(n^2)$ $\quad$ $O(n \log^2 n)$

Division with remainder (of n-bit numbers)

$O(n^2)$ $\quad$ $O(n \log n \log\log n)$

Exponentiation (of n-bit numbers)

$(x, e, N) \longmapsto x^e \pmod{N}$ new

$\boxed{O(en^2) = O(2^n n^2)}$ BAD

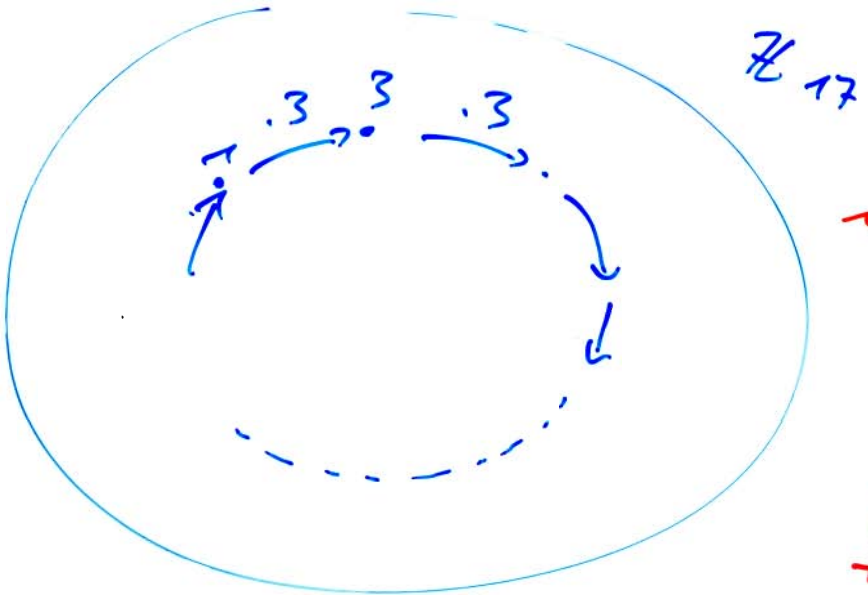
<u>Example</u> $3^{5000000}$ in $\mathbb{Z}_{17}$.

n	0	1	2	3	4	5	6	7	8
3^n	1	3	9	10	-4	5	-2	-6	-4

$\cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3$

	8	9	10	11	12	13	14	15
	-1	-3	8	7	4	-5	2	6

	16
	1



x
$\downarrow$
$y = x^e$ in $\mathbb{Z}_N$
$\downarrow$
$z = y^d = x^{ed}$ in $\mathbb{Z}_N$

Hopefully: $x^{ed} = x$!?

Thus $3^{5000000} = 3^0 = 1$ in $\mathbb{Z}_{\underline{17}}$.

We were allowed to reduce the exponent modulo $\underline{16}$.

<u>OBSERVATION</u> We stay in class!

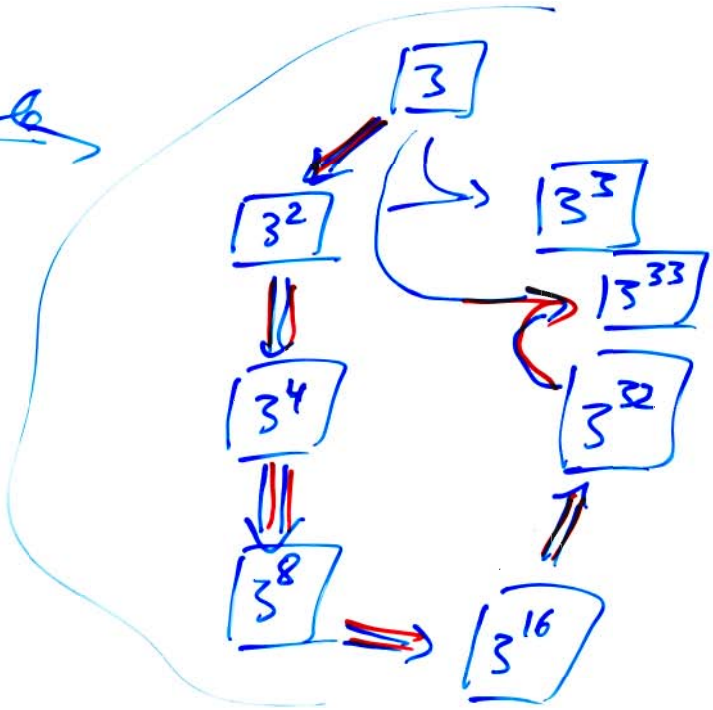
So every multiplication costs the same, we never deal with the integer $3^{5000000}$ or even 3^{16}.

Example 3^{33} in $\mathbb{Z}_{2^{16}+1}$.

Brute force: $1 \xrightarrow{\cdot 3} 3 \xrightarrow{\cdot 3} 9 \xrightarrow{\cdot 3} 27 \xrightarrow{\cdot 3} 81 \xrightarrow{\cdot 3} 243 \ldots$

~~steps~~ = 32 multiplications

Better? Yes $\xrightarrow{\text{example}}$



General solution

Repeated squaring
(Square and multiply)

Write the exponent in binary,

e.g. $42 = \underline{101}010_2$ to calculate x^{42}

we proceed like this:
(exponents in binary)

x^{1}
x^{10}
x^{100}
x^{101}
x^{1010}
x^{10100}
x^{10101}
x^{101010} done!

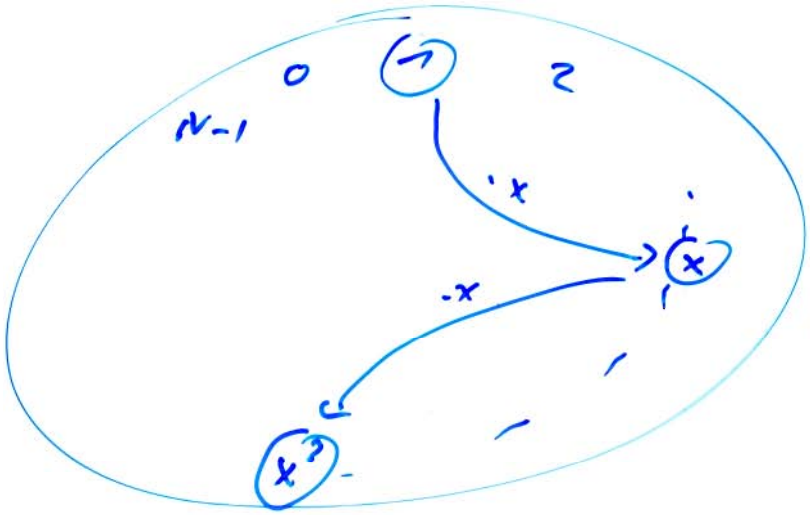
~~Time~~ Time: the exponent is an n-bit number

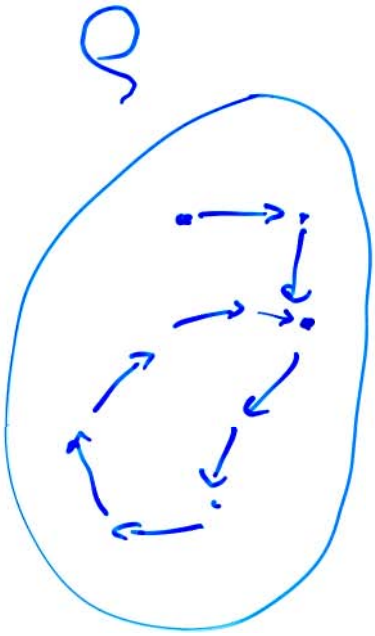
$O(n)$ multiplications.

So: $(\underbrace{x, e, N}_{\text{each n-bit number}}) \longmapsto x^e \pmod{N}$ needs $O(n \cdot n^2) = O(n^3)$ bit operations.
rem

„Cycling"

If we repeat multiplying with a number x in $\mathbb{Z}_N$, do we always end up in a cycle?





Since there only finitely many (namely N) elements we must meet an earlier seen number sooner or later from that point on we cycle...

Question: when does that happen and how long is the cycle?

First: after $\leq N$ steps and the length of the cycle $\leq N$.

24.10.06

8

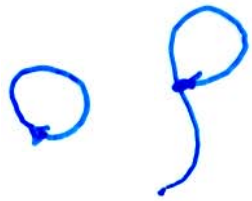
Examples

$\mathbb{Z}_3$: $x = -1$

n	0	1	$\boxed{2}$
x^n	1	-1	1

$\mathbb{Z}_4$: $x = -1$

n	0	1	$\boxed{2}$
x^n	1	-1	1



$\mathbb{Z}_5$: $x = 2$

n	0	1	2	3	$\boxed{4}$
x^n	1	2	-1	-2	1

$\mathbb{Z}_6$: $x = 2$

n	0	1	2	3
x^n	1	2	-2	2

$\boxed{2}$

$x = -1$

n	0	1	$\boxed{2}$
x^n	1	-1	1

$\mathbb{Z}_7$: $x = 2$

x^n	1	2	4	1

$x = -2$

$(-2)^n$	1	-2	4	-1	2	-4	1

$\mathbb{Z}_{15}$:

$x = 2 \in \mathbb{Z}_N^\times$ 1, 2, 4, -7, 1

$x = 3$ 1, 3, -6, -3, 6, 3

5 1, 5, -5, 5

$-2 \in \mathbb{Z}_N^\times$ 1, -2, 4, 7, 1

$7 \in \mathbb{Z}_N^\times$ 1, 7, 4, -2, 1

$\mathbb{Z}_{15}^\times$?

0 no

± 1 yes

± 2 yes

± 3 no

± 4 yes

± 5 no

± 6 no

± 7 yes

N	3	4	5	6	7	15
repetition lengths observed	2	2	4	2	{3, 6}	{2, 4}
$\# \mathbb{Z}_N^\times$	2=3-1	2	4=5-1	2	6=7-1	8

Observation: the repetition length observed always divide $\# \mathbb{Z}_N^\times$ (number of units).

Actually, the units form a group! [Ex!]

A (commutative) group is a set (or an ∞ class) with one operation, say multiplication, and the axioms P A N I C

So: don't PANIC, it's simple.

What did above happens in a finite group. We perform $\cdot x$ repeatedly.

Thm (Lagrange)

Given a finite group G and an element $x \in G$ then $x^{\#G} = 1$.

Pf (for commutative case) Write down a list of all group members:

$$(1=)g_0, g_1, g_2, \ldots, g_{L-1}. \quad (*)$$

Multiply every element by x:

$$(x=)xg_0, xg_1, xg_2, \ldots, xg_{L-1}. \quad (**)$$

These lists contain up to order the same elements!

$(**) \subset (*)$: Because with x and g_i also $x \cdot g_i \in G$.

$(*) \subset (**)$: Consider g_2. Is it on the second list? Is $g_2 = x \cdot g_i$ for some i? Equiv. $\underbrace{x^{-1} g_2}_{\in G} = g_i$

Thus g_2 is on the second list!

28.10.06
10

So the lists are equal up to order.
Take their product! Because G is commutative we get:

$$g_0 \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_{L-1} = xg_0 \cdot xg_1 \cdot xg_2 \cdot \ldots \cdot xg_{L-1}$$

Now multiply by $g_0^{-1} g_1^{-1} g_2^{-1} \cdot \ldots \cdot g_{L-1}^{-1}$:

$$1 = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{L}$$

$$1 = x^L \quad \text{where } L = \# G. \quad \square$$

<u>Corollary</u> (Euler)
Suppose $N \geq 2$ and $x \in \mathbb{Z}_N^\times$.
Then
$$x^{\varphi(N)} = 1$$
where
$$\varphi(N) = \# \mathbb{Z}_N^\times$$
Euler totient function. $\square$

<u>Corollary</u> (~~[illegible]~~ The little Fermat theorem)
Suppose p is prime number,
and $x \in \mathbb{Z}_p^\times$.
Then
$$x^{p-1} = 1. \quad \square$$

<u>Corollary</u> If p is prime then for $x \in \mathbb{Z}_p$
we have
$$x^p = x. \quad \square$$

Consider some RSA numbers:

N	$3\cdot 5$	$3\cdot 7$	$5\cdot 7$	$11\cdot 13$
$\# \mathbb{Z}_N^\times$	8	12	24	120
L	8	12	24	120

$\# \mathbb{Z}_{21}^\times = \{ \cancel{0}, \pm 1, \pm 2, \cancel{\pm 3}, \pm 4, \pm 5, \cancel{\pm 6}, \cancel{\pm 7}, \pm 8, \cancel{\pm 9}, \pm 10 \}$.

<u>Conjecture</u> $\# \mathbb{Z}_{pq}^\times = (p-1)(q-1)$

L if p, q are different primes.

This actually is true!

Brute force: Distinguish elements by their gcd with $N = p\cdot q$:

gcd	#	
$p\cdot q$	1	(namely 0)
p	$q-1$	(namely $p, 2p, \dots (q-1)p$)
q	$p-1$	(namely $q, 2q, \dots, (q-1)q$)
1	rest!	

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

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

Corollary RSA is correct in most cases.

Pf Suppose $x \in \mathbb{Z}_N^\times$, i.e. $x \in \mathbb{Z}_N$ and $\gcd(x, N) = 1$,
i.e. x is not a multiple of p or q.

By Euler's theorem we have now that

$$x^{\# \mathbb{Z}_N^\times} = 1.$$

and we know $\# \mathbb{Z}_N^\times = L = (p-1)\cdot(q-1)$.

Further we have $de = 1$ in $\mathbb{Z}_L$,

i.e. $de = 1 + k \cdot L$ for some $k \in \mathbb{Z}$.

So

$$x^{ed} = x^{1+k\cdot L} = x \cdot \underbrace{(x^L)}_{=1}{}^k = x \cdot \underbrace{1^k}_{=1} = x.$$

$\square$

Chinese Remainder Theorem

24.10.06
13'

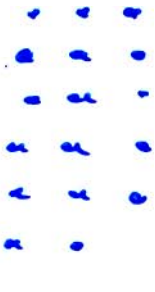
Task: in form of an example

school teacher with a certain number of pupils

in rows of 3 : 2 remain.

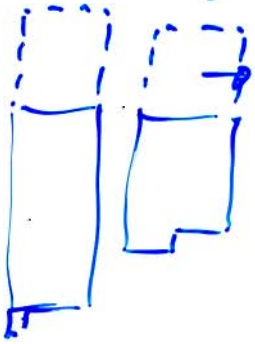
in rows of 4 : 1 remain.

in rows of 5 : ~~fits!~~ 1 remains!



How many pupils does (s)he have?

Say it's $\underline{a}$.



$$a = 5x + 1$$

$$\begin{cases} a = 4y + 1 \\ a = 3z + 2 \end{cases}$$

for some $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $z \in \mathbb{Z}$

$\rightarrow \quad 5x - 4y = 0$

$\rightarrow \quad \boxed{4y - 3z = 1} \longrightarrow$ EEA!

This works if $\gcd(4, -3) = 1$.

If 4 and -3 have gcd 1 then $4y - 3z = 7$ also has a solution.

Just use solution with r.h.s. $= 1$ and multiply by 7.

Ex:

4		1	0	
3	1	0	1	
1	3	1	-1	$\rightarrow 1 = 4 \cdot 1 + 3 \cdot (-1)$
0		-3	4 ✓	

$\boxed{4y = 3z}$

$y = 1, z = 1 \rightarrow a = \underline{\underline{12}}k + 5$

CRT

Given remainders $a_1, a_2, \dots, a_r \in \mathbb{Z}$
and moduli $m_1, m_2, \dots, m_r \in \mathbb{N}'_{>0}$
where ~~the moduli~~ each pair
of moduli has gcd 1
then there exists an integer $x \in \mathbb{Z}$
such that

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_r} a_r$$

and if x and y are two solutions
then $x-y$ is a multiple of $m_1 \cdot m_2 \cdot \dots \cdot m_r$.

Further: we can use the EEA to find
a solution for two moduli
and iterate that for arbitrarily
many conditions.

Pf It suffices to consider the case
$a_1 = 1,\ a_2 = 0$.

[Suppose

$$\begin{aligned} x_1 &\equiv_{m_1} 1 \\ x_1 &\equiv_{m_2} 0 \end{aligned} \qquad \begin{aligned} x_2 &\equiv_{m_1} 0 \\ x_2 &\equiv_{m_2} 1 \end{aligned}$$

$\rightarrow$ $a_1 x_1 + a_2 x_2 \equiv_{m_1} a_1$
$a_1 x_1 + a_2 x_2 \equiv_{m_2} a_2$.]

By the ~~EEA~~ we get

$$\boxed{\underbrace{s\,m_1}_{=:x_2} + \underbrace{t\,m_2}_{=:x_1} = \gcd(m_1,m_2) = 1}$$

then $\quad x_1 \equiv_{m_2} 0 \quad , \quad x_1 \equiv_{m_1} 1 - s\,m_1 \equiv_{m_1} 1$

Therefore:

$$\boxed{\left.\begin{array}{l} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \end{array}\right\} \Longleftrightarrow \quad x \equiv_{\underline{\underline{m_1 m_2}}} a_1 x_1 + a_2 x_2}$$

We skip:

$$\left.\begin{array}{l} x - y \equiv_{m_1} 0 \\ x - y \equiv_{m_2} 0 \end{array}\right\} \overset{\gcd = 1!}{\Longrightarrow} \quad x - y \equiv_{m_1 \cdot m_2} 0 \, .$$

$\square$

<u>Structural version</u>

$$\mathbb{Z}_{m_1 \cdot m_2} \xrightarrow{\cong} \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$$

$$x \bmod m_1 m_2 \longmapsto (x \bmod m_1 \, , \, x \bmod m_2)$$

$$(a_1 \, , \, a_2)$$

including structure!

$$\mathbb{Z}_{3 \cdot 5} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$$

0	$\longmapsto$	(0 ,	0)
1		(1 ,	1)
2		(2 ,	2)
3		(0 ,	−2)
4		(1 ,	−1)
5		(2 ,	0)
6		(0 ,	1)
7		(1 ,	2)
⋮		⋮	

In particular:

$$\mathbb{Z}_{m_1 m_2}^{\times} \cong \mathbb{Z}_{m_1}^{\times} \times \mathbb{Z}_{m_2}^{\times}$$

and thus

$$\# \mathbb{Z}_{m_1 m_2}^{\times} = \# \mathbb{Z}_{m_1}^{\times} \cdot \# \mathbb{Z}_{m_2}^{\times}$$

provided $\gcd(m_1, m_2) = 1$.

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

if p, q are different primes.

Now recall: for $x \in \mathbb{Z}_p$ we have $x^p = x$
and thus $x^{1 + k(p-1)} = x$.
in $\mathbb{Z}_p$.

Now, $de = 1 + k(p-1)(q-1)$ by def.

Thus for $x \in \mathbb{Z}_{pq}$ we find

$$x^{de} = x^{1 + [k(q-1)](p-1)} \equiv_p x$$
$$x^{de} = x^{1 + [k(p-1)](q-1)} \equiv_q x$$

$$\overset{CRT}{\Longrightarrow} x^{de} \equiv_{pq} x \quad (\text{in } \mathbb{Z}_{pq})$$

So: RSA is correct (in any case).

Summary

- RSA: Example

Choose keys: find two primes p, q.

How to? Choose random number and check if it's prime. Repeat if not.

First trial: $p = 12$

Is p prime? → Try the Little Fermat Theorem.

If p is prime then for any $x \in \mathbb{Z}_p^\times$ we have $x^{p-1} = 1$.

So let's try $x = 7$.

Now $7^{11} = 7^1 = 7 \neq 1$

Thus $p = 12$ is <u>not</u> prime.

$7^{10} = 1 = 7^2$ in $\mathbb{Z}_{12}$ (binary)

$\mathbb{Z}$ $\mathbb{Z}$

Second trial: $p = 11$.

Is it prime?

Let's try $x = 2$.

Now $2^{10} = 1$. Fine.

2^1

$2^{10} = 4$

$2^{100} = 5$

$2^{101} = -1$ in $\mathbb{Z}_{11}$

$2^{1010} = 1$

$1010_2 = 10 = 5+5$

This is not a proof but an indication.

If we are slightly more clever then we obtain the statement!

the found is prime with high probability

$\mathbb{Z}_{11} = 0, 1, 2, \dots 10$
$= 0, 1, 2, \dots 5, -5, -4, \dots -1$

Second prime: same process ... skip

$q = 5$

So we have $p = 11$, $q = 5$.

Thus
$$N = p \cdot q = 11 \cdot 5 = 55.$$
(size of the ring)

and
$$L = (p-1)(q-1) = 10 \cdot 4 = \underline{\underline{40}}$$
(repetition length)

Now we need $d, e \in \mathbb{Z}_L$ such that
$$de = 1.$$

To do that we choose d at random and (try to) compute e. If that fails: retry.

First trial: $d = \underline{\underline{2}}$.

→ Call EEA with $L, d = 40, 2$.

40		1	0
2	20	0	1
0		1	-20

check ok! ✓

But the gcd = 2 and so we fail.

Second trial: $d = 9$.

→ Call EEA 40, 9

40		1	0
9	4	0	1
4	2	1	-4
$\boxed{1}$	4	-2	9
0		9	-40

→ Check ok ✓

So: $1 = -2 \cdot 40 + 9 \cdot 9$

or: $1 = \underline{\underline{9}} \cdot 9$ in $\mathbb{Z}_{40}$.

→ $e = 9$.

→ Public key : $(N, e) = (55, 9)$
Secret key : $(N, d) = (55, 9)$

THROW AWAY ALL OTHER DATA!

<u>Encrypt</u> $x = 11 \in \mathbb{Z}_{55}$

public key : $(N, e) = (55, 9)$

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

$= 11^9$ in $\mathbb{Z}_{55}$ ...

$= 11$

$1001_2 = 9$ | 11^1, $11^{10} = 11$, ⋮

<u>Decrypt</u> $y = 11 \in \mathbb{Z}_{55}$

secret key : $(N, d) = (55, 9)$

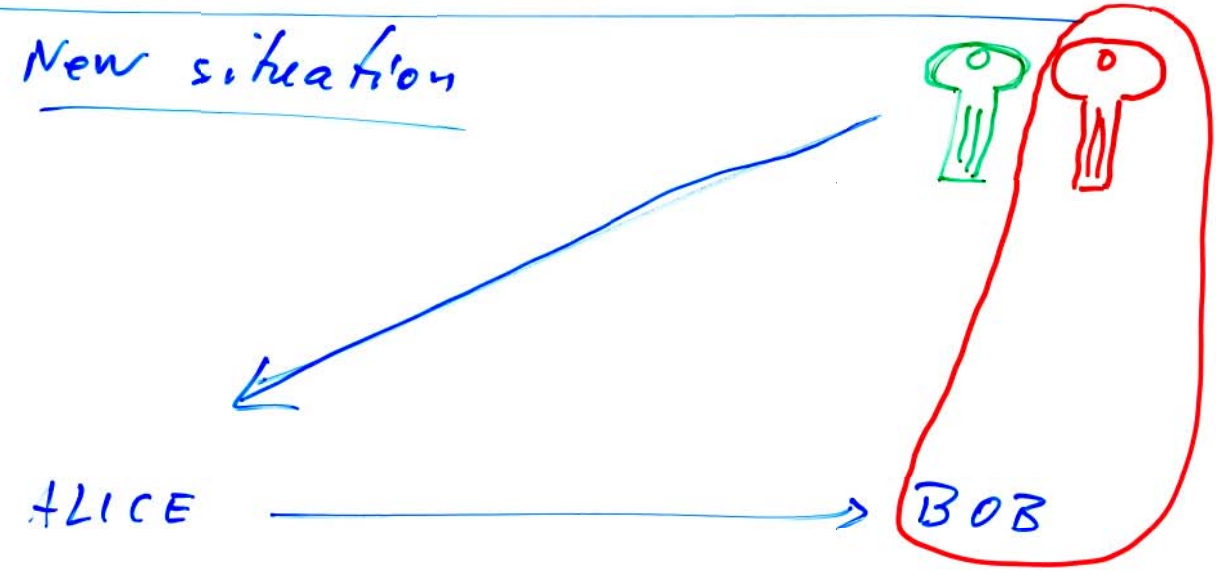
$z = y^d$ in $\mathbb{Z}_N$

$= 11^9$ in $\mathbb{Z}_{55}$

$= 11$

Note: $z = x$.

<u>New situation</u>



Summary cont'd

- Integers mod N, $\mathbb{Z}_N$
- Lagrange, Euler, Fermat
- Chinese Remainder Theorem
- Extended Euclidean Algorithm

we used this to prove that RSA is correct.

⌜ Pf I: Euler: $x^{\#\mathbb{Z}_{pq}^\times} = 1$ (mostly)
CRT → Adhoc: $\#\mathbb{Z}_{pq}^\times = (p-1)(q-1) = L$ } $\to x^L = 1$

By definition $de = 1 + k \cdot L$

$$x^{ed} = x^{1+k\cdot L} = \dots = x. \quad \triangle$$

Pf II: Little Fermat: $x^p = x$ in $\mathbb{Z}_p$,
$x^q = x$ in $\mathbb{Z}_q$.

Thus $x^{1+\ell(p-1)} = x$ in $\mathbb{Z}_p$,
$x^{1+\ell(q-1)} = x$ in $\mathbb{Z}_q$.

So $x^{ed} = x^{1+\underbrace{k(q-1)}(p-1)} = x$ in $\mathbb{Z}_p$

and $x^{ed} = x^{1+\underbrace{k(p-1)}(q-1)} = x$ in $\mathbb{Z}_q$.

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

so $x^{ed} = x$ in $\mathbb{Z}_{pq}$. $\square$ ⌟

- Repeated squaring
(Square and multiply)

In particular: $3^{5000002}$ in $\mathbb{Z}_{101}$ ⌜ Fermat, Euler $= 3^2 = 9$. ⌟

Side Chapter

Polynomials

2^x ? No. $x^{4.2}+17$? No.

$\sqrt{x}+2$? No. x^7+x^2+5 ? Yes!

A polynomial is an expression built from
- numbers and
- variables / indeterminates

by addition and multiplication.

Let's consider numbers from $\mathbb{Z}_2$.

How do we operate?

$a = x^7+x^4+x^3+1 \xrightarrow{\text{store}} 10011001$

$b = x^3+x+1 \xrightarrow{\text{store}} 00001011$

$$a+b = x^7+x^4+\underbrace{(1+1)}_{=0}\cdot x^3+x+0$$

$$= x^7+x^4+x. \xrightarrow{\text{store}} 10010010$$

XOR

$$a\cdot b = x^{10}+x^8+x^7+x^7+x^5+x^4+x^4+x^3+x^3+x+1 = x^{10}+x^8+x^6+x^5+x+1$$

$\xrightarrow{\text{in the above repr.}}$

$$\begin{array}{r} 10011001000 \\ \underline{00000000000} \\ 100110010 \\ 10011001 \\ \hline 10101100611 \end{array}$$

!

NO CARRY!

Division with remainder?

25.10.06

6

degree 3 > 1 degree

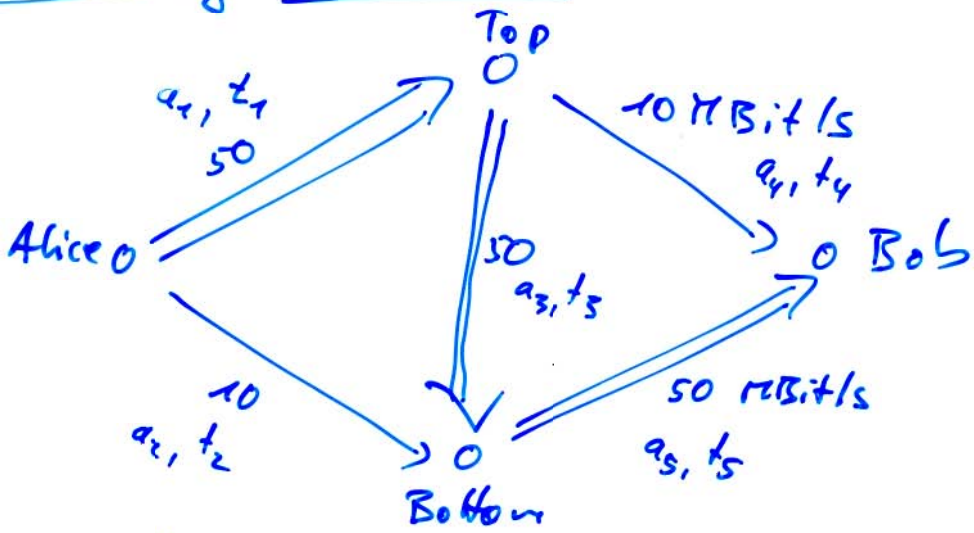
$$(x^{10} + x^7 + 1) = (x^7 + x^5 + x^3 + x^2 + x) \cdot \underbrace{(x^3 + x + 1)}_{\text{dividend}} + \underbrace{(x + 1)}_{\text{remainder}}$$

$$\begin{array}{l}
-(x^{10} + x^8 + x^7) \\
\hline
x^8 + 1 \\
-(x^8 + x^6 + x^5) \\
\hline
x^6 + x^5 + 1 \\
-(x^6 + x^4 + x^3) \\
\hline
x^5 + x^4 + x^3 + 1 \\
-(x^5 + x^3 + x^2) \\
\hline
x^4 + x^2 + 1 \\
-(x^4 + x^2 + x) \\
\hline
x + 1
\end{array}$$

remainder should be somehow „smaller" than the dividend.

→ Look at the <u>degree</u>!

Streaming video



Question: How to distribute the large data amount so that it reaches Bob best?

Requirement: all packets use the same time!
Necessary for streaming because the information must arrive (more or less) in the correct order.

Amount of data along a connection: a_i
Time to transmit it : t_i.

$\rightarrow$ edge conditions

$$\begin{cases} a_1 = 50 \cdot t_1 \\ a_2 = 10 \cdot t_2 \\ a_3 = 50 \cdot t_3 \\ a_4 = 10 \cdot t_4 \\ a_5 = 50 \cdot t_5 \end{cases}$$

...

Let's only use units: MBit and sec

path conditions
$$\begin{cases} t_1 + t_4 = T \\ t_1 + t_3 + t_5 = T \\ t_2 + t_5 = T \end{cases}$$
given constant, say $T = 1$ sec.

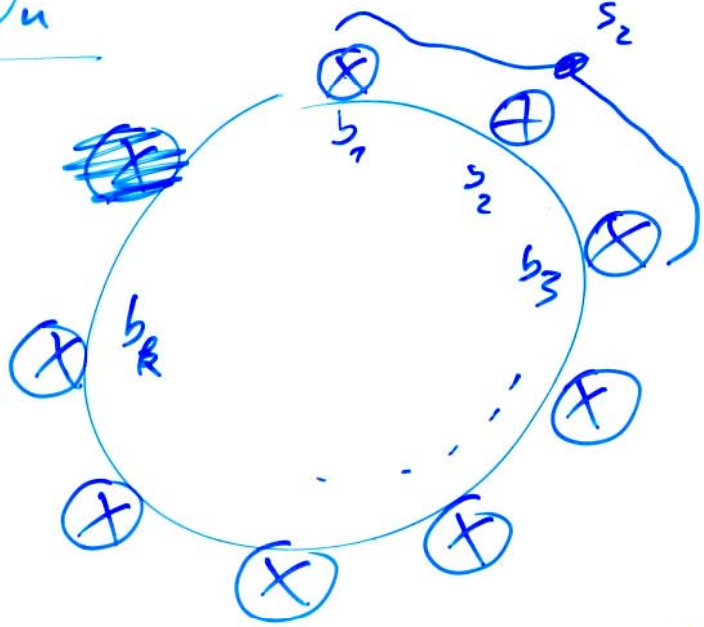
node conditions
$$\begin{cases} a_1 = a_3 + a_4 & \text{(Top)} \\ a_2 + a_3 = a_5 & \text{(Bottom)} \\ a_1 + a_2 = a_4 + a_5 & \text{(Alice / Bob)} \end{cases}$$

Only the time variables shall stay, so we use the edge conditions to describe the a_i:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 50 & 0 & -50 & -10 & 0 \\ 0 & 10 & 50 & 0 & -50 \\ -50 & -10 & 0 & 10 & 50 \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \end{bmatrix} = \begin{bmatrix} T \\ T \\ T \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

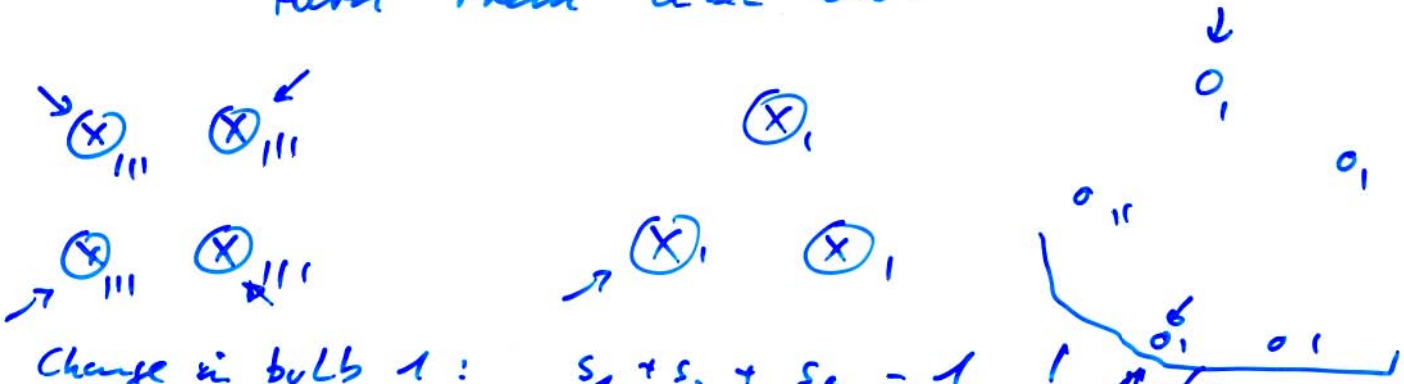
Find $t_1, \dots, t_5 \in \mathbb{Q}$!

Lights On



for each bulb there is a switch which changes the on/off state of the bulb and its two neighbours.

Goal: if at the beginning all bulbs are turned off, turn them all on!



Change in bulb 1: $s_1 + s_2 + s_k = 1$! And so on...!

$$\begin{bmatrix} 1 & 1 & 0 & \cdots & & 0 & 1 \\ 1 & 1 & 1 & 0 & \cdots & & 0 \\ 0 & 1 & 1 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & \ddots & \ddots & 1 \\ 0 & & & & & & \\ 1 & 0 & \cdots & & & 0 & 1 \; 1 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_k \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \quad \text{in } \mathbb{Z}_2 \; ?$$

→ Linear Algebra

25.10.06
10

How to solve linear systems of equations?

Example over $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 2 & 0 & 3 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 2 & 4 \\ 0 & 1 & 0 & 1/2 \end{bmatrix} \cdot \begin{bmatrix} x_1\ (4) \\ x_2\ (2) \\ x_3\ (0) \\ x_4\ (1) \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \quad x_1 + 2x_3 + 4x_4 = 3$$

elementary operations:

- exchange two rows
- multiply a row with an invertible number
- add any multiple of a row to another row

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

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

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

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

Gauß elimination

Goal: ① unit matrix on the left

Gauß-Jordan-Algorithm

or ② left matrix in form

Gauß elimination

$$\left[\begin{array}{cccccc} 1 & * & \cdots & * & * & * \\ 0 & 0 & \cdots & 0 & 1 & * \cdots * \\ \vdots & & & \vdots & 0 & 1 \quad * \\ & & & & \vdots & \ddots \\ 0 & & & 0 & 0 & 1 \ * \end{array}\right]$$

That's it.

No solution because the last line says: $0x_1 + 0x_2 + 0x_3 + 0x_4 = 1$ ↯.

In the green case:

$x_4 = 1$

$x_3 = 4 - 4 \cdot x_4 = 0$

$x_2 = 2 - x_3 = 2$

$x_1 = 1 - 2x_2 - 3x_4 = 4$.

So $x = [4, 2, 0, 1]^T$.

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

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

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

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

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

Gauß-Jordan-Algorithm

→ Nicer result

→ But numerically less stable!

Further questions:

- How fast (slow) is this?
- Can we decide how many solutions there are?
- We can multiply matrices.
  Then: can we find an inverse matrix for a given square matrix? When? How?

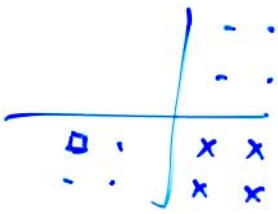
Cost: $\underbrace{O(n^3)}_{\text{operation in the ground field}}$ for both Gauß-elimination and Gauß-Jordan-Algorithm.

Better? It can be done in the same order of magnitude as matrix multiplication. So if m.m. can be done faster we gain sth.

Strassen (≈ 1970) Gauß-elimination is <u>not</u> optimal

$$\rightarrow \quad O(n^{\underset{\log_2 7}{2.83}})$$

T



Multiply 2x2 matrices: 8 multiplications

Strassen: 7 multiplications

Usually: $T(2^k) = 8 \cdot T(2^{k-1}) + \dots$

$$\rightarrow T(2^k) \approx 8^k \approx (2^k)^3$$

Here:

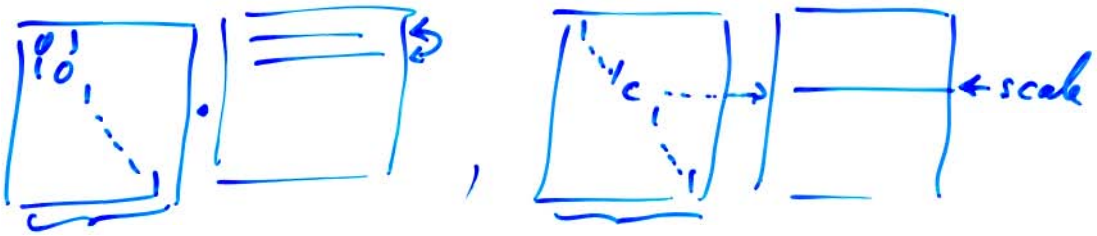
$$T(2^k) = 7 \cdot T(2^{k-1}) + \dots$$

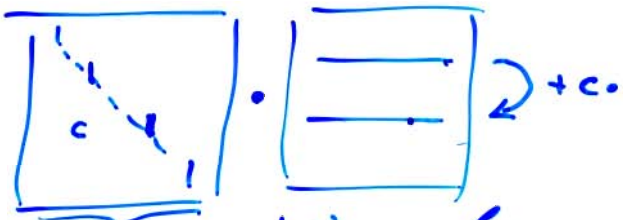
$$\rightarrow T(\underbrace{2^k}_{n}) \approx 7^k = (\underbrace{2^k}_{n})^{\log_2 7}$$

Record: $O(n^{2.38})$, Coppersmith & Vinograd '90

Observation on the structure of gaussian elimination

Any row operation can be described as multiplication with an appropriate matrix from the left.





lower triangular

We start with a problem like

$$A\,x = b$$

$$\underbrace{\overbrace{M_k \cdots M_3 M_2 M_1 A}^{L}}_{\text{until: special form}}\, x = M_k \cdot \ldots \cdot M_1 b$$

<u>Thm</u> For any square matrix A there exists a permutation matrix P and a lower left triangular matrix L and an upper right triangular matrix R such that

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

$\triangle$

Now, solving $Ax = b$
is equivalent to solving

$$PAx = Pb$$
$$PA = L(Rx)$$

ie.
$$Ly = Pb$$
and
$$\boxed{Rx = y}$$

Look more closely:

$$R = \begin{bmatrix} 1 & * & * & * & & * & * & * & * & * \\ & & & & 1 & * & * & & * & * \\ & & & & & & & 1 & * & * \\ & & & & & & & & & \\ & & & 0 & & & & & & \end{bmatrix}$$

It may happen that there is no solution, and we see that in the "lower" coordinates of y.

$$\begin{bmatrix} 1 & \cdots & & \\ & 1 & \cdots & \\ & & 1 & \cdots \\ & & & \\ & & 0 & \end{bmatrix} = \begin{bmatrix} * \\ * \\ * \\ \\ \neq 0 \end{bmatrix}$$

if this is not zero there is no solution and vice versa.

How „many" right hand sides have a solution?

There is a family of r.h.s. with r parameters where

$$r = \#\text{ non-zero rows in } R.$$
$$=: \operatorname{rank} A.$$
$$= \dim(\operatorname{im} A)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} * \\ 0 \\ 0 \end{bmatrix}$$

Now, if the given b is in the image
$\operatorname{im} A = \{ Ax \mid x \in k^n \}$,
then $Ax = b$ has a solution.

So then $A' = (A|b)$ gives me a matrix
with same image: $\operatorname{im} A = \operatorname{im}(A|b)$.

Otherwise, if no ~~sol~~ solution exists
then $\underbrace{\operatorname{im} A}$ $\neq$ $\operatorname{im}(A|b)$

So there exists a solution
iff $\operatorname{rank} A = \operatorname{rank}(A|b)$.

How many solutions are there? How many parameters do we need to describe all solutions?

$$r\left\{\underbrace{\begin{bmatrix} 1 & * & \cdots & & & 1 & * & \cdots & & & 1 & * & \cdots \\ & & & & & & & & & & & & \\ | & & & & & | & & & & & | & & \end{bmatrix}}_{n}\right. x = y = \begin{bmatrix} * \\ * \\ * \\ 0 \end{bmatrix}$$

Answer: $\underline{\#(\text{col's of } A) - \operatorname{rank} A}$.

Open:
- Invert a square matrix.
- Criterion when that is possible.

Task: Given a square matrix A.
Find a matrix X with $AX = \mathbb{1}$

How: Solve the lin. sys.; $[A \mid \mathbb{1}]$ $\qquad \mathbb{1} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$

Result of Gauß-Jordan will be $[\mathbb{1} \mid X]$ if possible

or $\left[\begin{matrix} * \\ 0 \dots 0 \end{matrix} \,\middle|\, * \right]$ otherwise

Define: determinant of A

→ Properties: $\det \mathbb{1} = 1$,

$\det(A \cdot B) = \det A \cdot \det B$

$$\det \begin{pmatrix} a_1 & & * \\ & a_2 & \\ 0 & & \ddots \; a_n \end{pmatrix} = a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

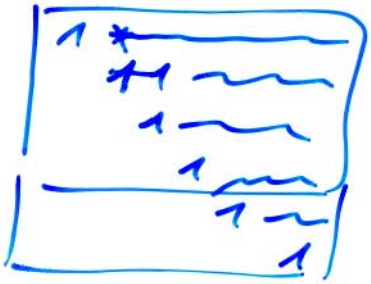
$$\det \begin{pmatrix} a_1 & & 0 \\ & a_2 & \\ * & & \ddots \; a_n \end{pmatrix} = a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

By Gaußian elimination we obtain

$$PA = LU$$

so
$$\det A = \det(P^{-1} L R)$$
$$= \underbrace{\det(P^{-1})}_{\pm 1} \cdot \underbrace{\det L}_{\text{product of scalings}} \cdot \underbrace{\det R}_{\text{either } 0 \text{ or } 1}$$

In fact: $\det R = 1$ iff $\operatorname{rank} R = n$ $\overset{\shortparallel}{\operatorname{rank} A}$



otherwise $\det R = 0$

So:

$$\boxed{\begin{array}{c} \det A = 0 \text{ iff } \operatorname{rank} A < n \\ \hline A^{-1} \text{ exists iff } \det A \neq 0 \end{array}}$$

Probability

26.10.06
1

→ error correction (e.g. playing music, sending data via satellite, ...)

→ modelling physics

→ randomness in algorithms
- (in RSA & other crypto) in order to hide certain information, to generate secrets
- to simulate difficult reality ↯ - forecasting (weather)
- to test whether a number is prime

... „algorithm is fast" = ?
→ worst case complexity
→ average case complexity
⇝ What means „average"?
→ only few bad cases

→ analysis of algorithms
- inputs are often somehow random
  the distribution influences e.g. the average running time
  finding a distribution that models reality may be difficult.

? decision making

→ gambling & games
- coin tossing
- dice
- cards

Questions: • What is the winning probability?
• What is the expected win? (average)

Monty Hall Problem

behind two of is a goat: you loose.
behind one is large win, eg. a car.

- You choose one door. (prob(car) = $\frac{1}{3}$.)
- The quiz master opens one of the other doors with a goat behind it.
- You may now either stay at the chosen door or switch to the remaining one.

Question: What should you do (in order to optimize your winning probability) ?

Factoring

Pollard-ρ

You are given a number N (without small factors) and it is not prime. <1000000

You want to compute a factor of N.

Solution proposed

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

eg. $f(x) = x^2+1$,

and a seed $x_0 \in \mathbb{Z}_N$.

Compute

$$x_0,$$
$$x_1 = f(x_0)$$
$$x_2 = f(x_1)$$
$$x_3 = f(x_2)$$
$$\vdots$$

until two of these numbers coincide modulo a factor: $\gcd(x_i - x_j, N) > 1$.

Algorithm

Input: N.

Output: either a factor p of N or FAIL.

1. $x_0 \in_R \mathbb{Z}_N$, $y_0 := x_0$, $i := 0$.
2. Repeat
3. $\quad i := i+1$; $x_i := f(x_{i-1})$, $y_i := f(f(y_{i-1}))$.
4. Until $p := \gcd(x_i - y_i, N) > 1$
5. If $p = N$ then return FAIL
   else return p.

② birthday paradox

① running of a randomly terminated loop

Heuristically

Expected running time: $O(\sqrt[4]{N})$

26.10.06
(10)

Running time of a randomly terminated loop

We have an algorithm like:

1. Repeat
2. Something
3. Until condition holds.

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

What the expected number of iterations?

(Same question:

How often do I need to throw a coin until heads turns up on average? (prob $= \frac{1}{2}$)

How often do I need to throw a die until a six falls (on average)? (prob $= \frac{1}{6}$),

Answer: 42.

Language for probability theory

finite probability space

for simplicity

U finite set (~~events~~ outcomes, possible outcomes)

$P : U \longrightarrow [0,1]$

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

Example coin tossing:

$U = \{ \text{head}, \text{tails} \}$

$P(\text{head}) = \frac{1}{2}$, $P(\text{tails}) = \frac{1}{2}$

for a fair coin.

real coin: $U = \{ \text{head}, \text{tails}, \text{rim} \}$

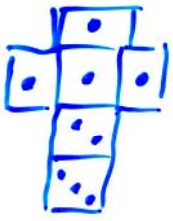
$P(\text{head}) = P(\text{tails}) = 0.4999$

$P(\text{rim}) = 0.0002$

rolling dice:

$$\left.\begin{array}{l} U = \{1,2,3,4,5,6\} \\ P(u) = \frac{1}{6} \end{array}\right\} \text{fair die}$$

special die



$U = \{ \bullet, \bullet\bullet, \bullet\bullet\bullet \}$

$P(\bullet) = 4/6$, $P(\bullet\bullet) = 1/6$, $P(\bullet\bullet\bullet) = 1/6$.

An <u>event</u> is a set of outcomes.

Eg. prob (The die rolls on an even number)

$= \text{prob}(\{2,4,6\}) = \frac{1}{2}$

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

We define for $E \subset U$

$$\text{prob}(E) = \sum_{u \in E} P(u).$$

Eg. prob(die gives a number less than 5)

$= \text{prob}(\{1,2,3,4\})$

$$= \sum_{u \in \{1,2,3,4\}} P(u)$$

$= P(1) + P(2) + P(3) + P(4).$

<u>Names</u>: P is called <u>distribution</u>,

prob is <u>probability (fn)</u>.

A distribution is <u>uniform</u>

iff $P(u)$ is the same for all $u \in U$.

Null event : $\emptyset = \{\} \subset U$. $\text{prob}(\emptyset) = 0$.

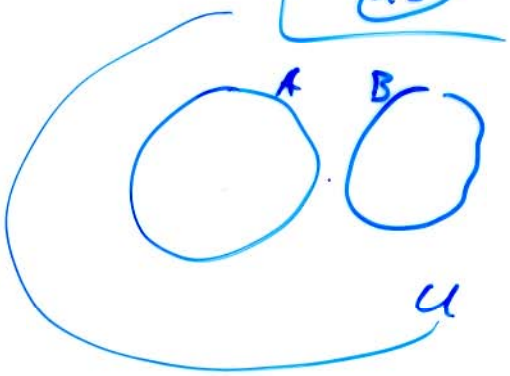
Always event : $U \subset U$. $\text{prob}(U) = 1$.

Suppose A, B are two events.

First, assume $A \cap B = \emptyset$,

then $\text{prob}(A \dot\cup B)$

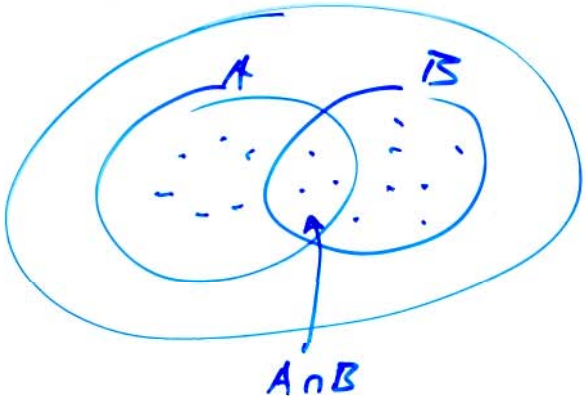
$= \text{prob}(A) + \text{prob}(B)$



Now, in general:

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

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



Further:

$$\text{prob}(\underbrace{U \setminus A}_{\text{"not } A\text{"}}) = 1 - \text{prob}(A)$$

⌜ We find $\text{prob}(A) + \text{prob}(U \setminus A)$

$$= \text{prob}(\underbrace{A \cup (U \setminus A)}_{U}) = 1.$$ ⌟

¿ $\text{prob}(A \cap B) = \text{prob}(A) \cdot \text{prob}(B)$?

<u>Ex</u> Fair die $A = \{2,4,6\}$, $B = \{4,5,6\}$

$\text{prob}(A) = 1/2$

$\text{prob}(B) = 1/2$

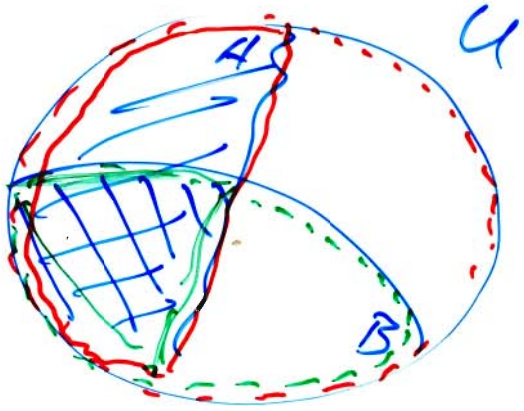
$\text{prob}(\underset{\{4,6\}}{\underset{\shortparallel}{A \cap B}}) = \frac{1}{3} \neq \frac{1}{2} \cdot \frac{1}{2}$.

Def Two events A, B with

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

are called <u>independent</u>.

Conditional probabilities:



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

only if $\text{prob}(B) \neq 0$.

read: the probility of A given that B already happened

So: two events A, B are independent if

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

Ex fair die $A = \{2, 4, 6\}$, $B = \{1, 2\}$

$$\text{prob}(A \mid B) = \frac{\text{prob}(A \cap B)}{\text{prob}\, B} = \frac{\text{prob}(\{2\})}{\text{prob}(\{1, 2\})}$$

$$= \frac{1/6}{2/6} = \frac{1}{2}.$$

and here also $\text{prob}(A) = 1/2$, so these A, B are independent.

Ex Monty Hall problem:

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

$P(1) = 1/3, \quad P(2) = 1/3, \quad P(3) = 1/3.$

Say Monty Hall opens door 3 and there is a goat. So: $B = \{1, 2\}$ remains.

$$\text{prob}(1 \mid B) = \frac{\text{prob}(\{1\} \cap B)}{\text{prob } B} = \frac{1/3}{2/3} = \frac{1}{2},$$

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

From this it seems not to make a difference whether we switch or not.

⚠ But: this does <u>not</u> describe the show.

Right answer:

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

$\text{prob}(\text{car with switch}) = 2/3$

Random variable (r.v.)

<u>Def</u> A r.v. is a function

$$X : U \longrightarrow \mathbb{R}$$

might also be something more general

eg.

X = outcome of rolling a die
where U = set of possible situations including table, hand, the die cube, positions and movements of all the particles involved
...

The only thing that I need to calculate further things are the probabilities of the set

$$\{u \mid X(u) = 1\}, \quad =: \{X = 1\}$$

$$\{u \mid X(u) = 2\} \qquad X = 2$$

$$\vdots \qquad\qquad \vdots$$

$$\{u \mid X(u) = 6\} \qquad X = 6$$

so $\quad \text{prob}(X = 1) = \text{prob}(\{u \mid X(u) = 1\})$

$\overset{!}{=} 1/6$ for a fair die.

then we can calculate $\text{prob}(X \text{ even})$

$= \text{prob}(X = 2) + \text{prob}(X = 4) + \text{prob}(X = 6)$.

the function

$$\left\{\begin{matrix}\text{possible outcomes}\\ \text{of } X\end{matrix}\right\} \longrightarrow \mathbb{R}$$

$$x \longmapsto \text{prob}(X=x)$$

is the <u>distribution</u> of X.

<u>Define</u> the expected value

$$E(X) := \sum_{x\in\mathbb{R}} x \cdot \text{prob}(X=x)$$

Actually this sum is finite...

<u>Ex</u> X = age of a randomly selected member of our class

then $E(X)$ = average age.

not important

<u>Ex</u> fair die, $X(u) = u$ on $U = \{1,2,3,4,5,6\}$
$P(u) = 1/6$ for $u \in U$.

then $\boxed{P(X=x) = 1/6 \text{ for } x \in \{1,2,3,4,5,6\}}$

this is essential.

there: $E(X) = 1\cdot 1/6 + 2\cdot 1/6 + 3\cdot 1/6 + \dots + 6\cdot 1/6$

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

$u \mapsto (X(u) - EX)^2$ is a r.v.

Also often interesting: variance

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

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

Def Two random variables X, Y (on the same probability space) are <u>independent</u> iff

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

for all x, y.

Back to the running time:

<u>Algorithm</u>

0. $i := 0$
1. repeat
2. $\quad i := i + 1$
3. $\quad x_i \in_R \mathbb{Z}_{42}$
4. until $x_i = 0$

$x_0, x_1, x_2 \ldots\ldots$ ϕ 0!

What are the r.v.s?

For each $i \in \mathbb{N}$ we have a r.v.

$$X_i \quad \text{with} \quad \text{prob}(X_i = x) = \frac{1}{42}$$

for each $x \in \mathbb{Z}_{42}$.

Actually, they are (pairwise) <u>independent</u>.

The distribution of the fifth r.v. X_5 does not depend on the outcome of the previous ones, X_1, X_2, X_3, X_4.

This defines: $\text{prob}(X_1 = 3, X_5 = 7) =$

$$\text{prob}(X_1 = 3) \cdot \text{prob}(X_5 = 7) = \frac{1}{42^2}.$$

Let $S_k = i$

iff $X_1 \neq 0, X_2 \neq 0, \dots, X_{i-1} \neq 0, X_i = 0.$

ie. S is the stopping time

What we want is the expected value of this S.

$$E(S) = \sum_i i \; \text{prob}(S = i)$$

Now $\text{prob}(S = i)$

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

small proof ... Ex!

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

$$= \left(1 - \frac{1}{42}\right)\left(1 - \frac{1}{42}\right) \cdots \left(1 - \frac{1}{42}\right) \cdot \frac{1}{42}$$

$$= \underbrace{\left(1 - \frac{1}{42}\right)}_{=:q}^{i-1} \cdot \underbrace{\frac{1}{42}}_{=:p}$$

So $$E(S) = \underbrace{\sum_{i \geq 0} i \cdot q^{i-1}}_{1/p^2} \cdot p \overset{\text{analysis}}{=} \frac{1}{p}.$$

In particular: $$E(S) = \frac{1}{1/42} = 42.$$

$\square$

Your questions:

- birthday problem
- r.v.
- Can one win in the casino?

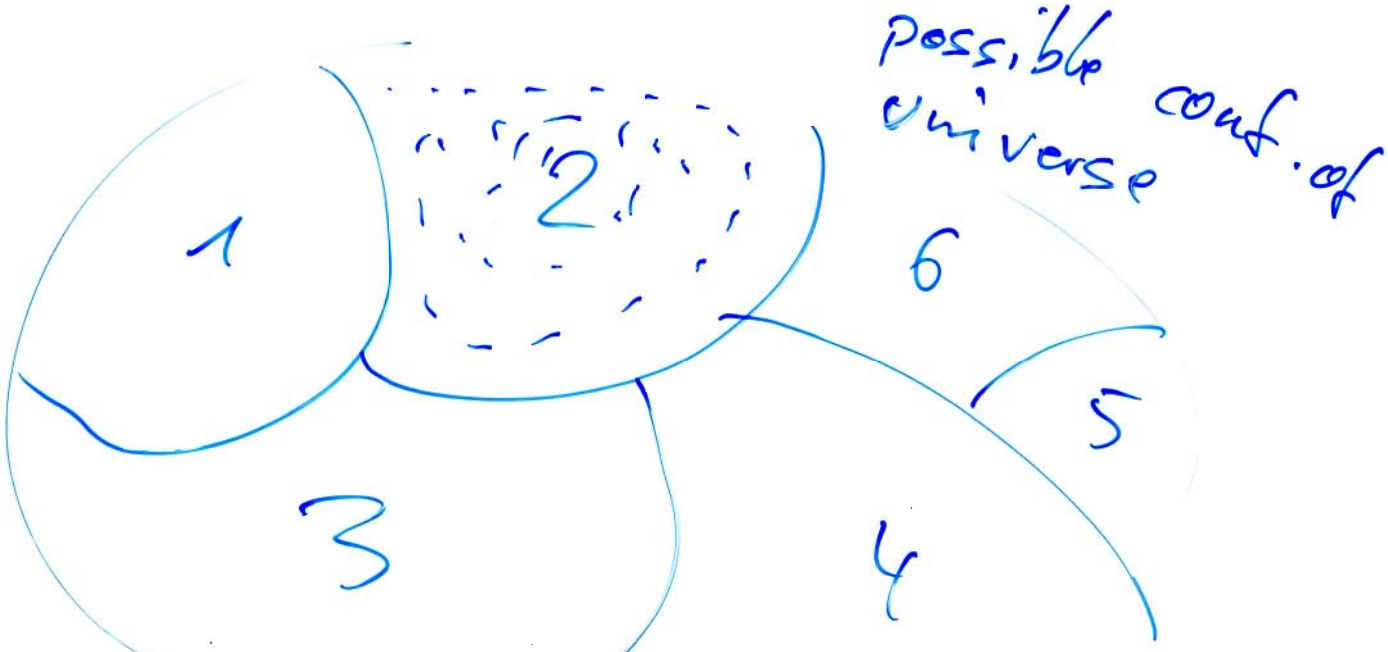
Estimated win for the doubling strategy is:

$$E(\text{win if we stop after } k \text{ rounds}) = \frac{1}{2}\cdot 1€ + \frac{1}{4}\cdot 1€ + \frac{1}{2^3}\cdot 1€ + \dots + \frac{1}{2^k}\cdot 1€$$

$$= \frac{1}{2^k}\,(\underbrace{1+2+\dots+2^k}_{\frac{2^{k+1}-1}{2-1}})\,€$$

$$= \left(\left(1-\frac{1}{2^k}\right) - 2 + \frac{1}{2^k}\right) €$$

$$= -1\,€$$



$$X : U \longrightarrow \mathbb{R}$$

$$\text{prob}(X=2) = \text{prob}\{u \mid X(u)=2\} = \sum_{u:\,X(u)=2} P(u).$$

Birthday paradox

~~Let $X_1, \dots, X_k$ r.v. with n possible outcomes~~

$p := \text{prob}(\, X_1, \dots, X_k$ there is twice the same value $)$

Where $X_1, \dots, X_k$ are r.v.

with the same set $\{1, \dots, n\}$ of possible values

and $\text{prob}(X_i = x) = \frac{1}{n}$

and $X_1, \dots, X_k$ are independent.

It's easier to calculate

$$
\begin{aligned}
1-p &= \text{prob}(\, X_1, \dots, X_k \text{ are all } \underline{\text{different}}\,) \\
&= \text{prob}(\, X_1 \text{ is anything}, \\
&\qquad X_2 \text{ is anything but not } X_1 : X_2 \neq X_1, \\
&\qquad X_3 \neq X_1,\ X_3 \neq X_2 \ : X_3 \notin \{X_1, X_2\} \\
&\qquad \vdots \\
&\qquad X_k \notin \{X_1, \dots, X_{k-1}\}\,) \\
&= \text{prob}(\, X_1 \text{ arb.}) \\
&\quad \cdot \text{prob}(X_2 \neq X_1 \mid X_1) \\
&\quad \cdot \text{prob}(X_3 \notin \{X_1, X_2\} \mid X_1 \neq X_2) \\
&\quad \vdots \\
&\quad \cdot \text{prob}(X_k \notin \{X_1, \dots, X_{k-1}\} \mid X_1, \dots, X_{k-1} \text{ are different})
\end{aligned}
$$

$$= 1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right)$$

$$\approx 1 - \underbrace{\left(\frac{1}{n} + \frac{2}{n} + \frac{3}{n} + \dots + \frac{k-1}{n}\right)}_{} + \underbrace{\frac{\dots}{n^2} - \frac{\dots}{n^3} + \dots}_{\text{small}}$$

So $\boxed{p \approx} \frac{1}{n} + \frac{2}{n} + \frac{3}{n} + \dots + \frac{k-1}{n}$

$$= \frac{k(k-1)}{2n} \approx \boxed{\frac{k^2}{2n}}$$

If now $k \approx \sqrt{2n}$ then p is near 1.

One can prove that the expected number of trials until a collision occurs is $O(\sqrt{n})$.

22.10.06

Some exercises

Number theory

① Calculate $3^{5000340087}$ rem 401

② • Generate a key pair for RSA with $p = 7$ and $q = 11$.

• Verify your key pair by encrypting $x = 2$ and decrypting again.

③ Prove that RSA is correct.

④ Determine x such that $x \equiv_7 1$ and $x \equiv_{13} 3$.

Linear algebra

⑤ Solve $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 3 & -1 \\ 1 & 0 & 2 \end{bmatrix} x = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ over $\mathbb{Z}_{11}$.

⑥ Invert the matrix $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ over $\mathbb{Z}_2$.

Probability

⑦ prob(eat an egg for breakfast) = 0.3,
prob(is an American) = 0.1
prob(egg | American) = 0.7

Determine prob(American | egg) = ?

⑧ What's the (a) probability space for Blackjack? Expected win?

⑨ What's the expected running time for playing in the lottery until you win? (Say 6 in 48...)

$x \equiv_7 1 \qquad x \equiv_{13} 3$

To solve this call EEA(13,7)

13		1	0
7	2	0	1
-1	-7	1	-2
0		7	-13

← Check ok ✓

$\underline{-1} = 1 \cdot 13 + (-2) \cdot 7$

$$\boxed{1 = \underbrace{(-1) \cdot 13}_{=: x_1} + \underbrace{2 \cdot 7}_{=: x_2}}$$

So now

$x_1 \equiv_7 1, \quad x_1 \equiv_{13} \underline{0}$

and

$x_2 \equiv_7 0, \quad x_2 \equiv_{13} 1$

$\cdot 1$, $\cdot 3$ $\Big\}$ +

$x := x_1 + 3x_2 \equiv_7 1 + 3 \cdot 0 = 1 \qquad x := x_1 + 3x_2 \equiv_{13} 0 + 3 \cdot 1 = 3$

So

$$x \equiv_{7 \cdot 13} \overbrace{(-1) \cdot 13}^{x_1} + 3 \cdot \overbrace{2 \cdot 7}^{x_2} = 39 .$$