RSA algorithm

How does it work?

- Choose two primes $p, q$, and large and randomly.
- Let $N = pq$, $L = (p-1)(q-1)$.
- Choose two numbers $e, d \in \mathbb{N} < L$ such that $ed = 1 \mod L$.
  (i.e., $\frac{ed - 1}{L} \in \mathbb{Z}$, $\frac{ed - 1}{L}$ divides $(ed - 1)$, $L \mid (ed - 1)$.)
- Now, $(N, e)$ is the public key, $(N, d)$ is the secret key.

Throw away any thing else!!!!!!

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

Based on integer factorization.
class "ring of integers modulo $N".

$\mathbb{Z}_N$

elements: $0, 1, 2, 3, ..., N-1$

operations:
- $+: a \mod_N b \equiv (a+b) \mod N$
- $\cdot: a \cdot b \equiv (a \cdot b) \mod N$
- $-: ...$

0, 1

axioms:

- **Commutative group (with +)**
  - Prop: $+, -$ are properly defined.
  - Assoc: $(a+b)+c = a+(b+c)$
  - Neutral: $a+0 = a = 0+a$
  - Inverses: $a+(-a) = 0 = (a+1)$
  - Commut: $a+b = b+a$

- **Commutative ring**
  - Prop: $\cdot$ is properly defined.
  - Assoc: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - Neutral: $a \cdot 1 = a = 1 \cdot a$
  - Distributive: $(a+b) \cdot c = a \cdot c + b \cdot c$

Then $0 \cdot a = 0$.

**Ex**:
Then

Proof

0 \cdot a = 0

\begin{align*}
0 \cdot a &= 0 \cdot (a + 0) \\
&= 0 \cdot a + 0 \cdot 0 \\
&= 0 \cdot a + 0 \\
&= 0 \cdot a \\
&= 0
\end{align*}

Examples \text{ (\S 26)}

4.5 = 6 \pmod{7}

4.5 = 20 \pmod{26}.

20 = 2 \cdot 7 + 6 \text{ remainder 6.}

2.3 = 0 \pmod{26}

4.5 = -1 \pmod{26} \text{ true}

\begin{align*}
&b = 0 \\
&b = 6 + 0
\end{align*}
Variation of the class

other element set: $\{-\lfloor \frac{N-1}{2} \rfloor, \ldots, -1, 0, 1, \ldots \lfloor \frac{N-1}{2} \rfloor\}$

$N = 7$: $-3, -2, -1, 0, 1, 2, 3$
$N = 4$: $-2, -1, 0, 1$

\[ \mathbb{Z} \xrightarrow{\text{mod}} \mathbb{Z}_N \]
\[ a \xrightarrow{\text{"a rem N"}} \frac{a}{a} \]

\[ \mathbb{Z} \rightarrow \mathbb{Z}_7 \]
4
4.4 = 16
4.4 = 2

\[ \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \]
\[ (a, b) \rightarrow a \text{ rem } b \]

\[ \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_6 \]
\[ (a, b) \rightarrow a \text{ mod } b \]
Multiplicative inverses

Example 2 in \( \mathbb{Z}_7 \):

What is \( x \) with \( 2 \cdot x = 1 \) in \( \mathbb{Z}_7 \)?

Here, \( x=4 \) is a solution: \( 2 \cdot 4 = 1 \) in \( \mathbb{Z}_7 \).

\[
\begin{array}{c|cccccc}
\mathbb{Z}_7 & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
x^1 & 1 & 2 & 3 & -3 & -2 & -1
\end{array}
\]

Problem Given \( x \) in \( \mathbb{Z}_N \),
find \( y \) such that \( x \cdot y = 1 \) in \( \mathbb{Z}_N \).

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 \( x = 2 \), \( N = 7 \).

\[
\begin{align*}
1 \cdot 2 + 0 \cdot 7 &= 2 \\
0 \cdot 2 + 1 \cdot 7 &= 7 \\
(-3) \cdot 2 + 1 \cdot 7 &= 1
\end{align*}
\]

\[
\frac{-8N+1}{x} = y
\]

\[
\frac{1015}{15} = 67 \quad \text{with division}
\]

\[
\frac{1015}{15} = 67 \cdot 15 + 8 \quad \text{quotient, remainder}
\]

Running time: \( O(n^2) \)
Example

\[ x = 142, \quad N = 349 \]

\[
\begin{align*}
0 \cdot x + 1 \cdot N &= 349 \\
1 \cdot x + 0 \cdot N &= 142 \\
(-2) \cdot x + 1 \cdot N &= 65 \\
6 \cdot x + (-2) \cdot N &= 12 \\
(-23) \cdot x + 11 \cdot N &= 5 \\
59 \cdot x + (-28) \cdot N &= 2 \\
\underline{(-142) \cdot x + 53 \cdot N} &= 1
\end{align*}
\]

\[ 349 \cdot x + (-142) \cdot N = 0 \quad \text{(Verification)} \]

Extended Euclidean Algorithm

Thus \( 142^{-1} = -145 \) in \( \mathbb{Z}_{349} \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>( x_i )</th>
<th>( a_i )</th>
<th>( s_i )</th>
<th>( t_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>349</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>142</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>65</td>
<td>2</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td></td>
<td>-2</td>
<td>5</td>
</tr>
</tbody>
</table>
Example \( x = 12, \ N = 70 \).

<table>
<thead>
<tr>
<th>( r_i )</th>
<th>( q_i )</th>
<th>( s_i )</th>
<th>( t_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>70</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>-2</td>
<td>-6</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>6</td>
<td>-3.5</td>
</tr>
</tbody>
</table>

We read off: \( 2 = (-1) \cdot 70 + 6 \cdot 12 \).

and no smaller result possible.

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

Theorem

(a) If the EEA finds a solution to \( y \cdot x + k \cdot N = 1 \) 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 \( \mathbb{Z}_N \).

Proof

(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 \( +1 \).
Go suppose the EEA terminates with $e = d$ and $y \cdot z + k \cdot N \neq \pm 1$.

And $\text{test} = 0$.

Note that $r_{i+1} = q_i \cdot r_i + r_{i-1}$ for all $i > 0$.

IBasis: $d = 1$:

We have $\gcd(r_i, d)$ and $\gcd(r_{i+1}, d)$.

We want $\gcd(r_{i-1}, d)$ and $\gcd(r_i, d)$.

$\frac{\gcd(r_i, d)}{\gcd(r_{i-1}, d)} \rightarrow \frac{\gcd(r_{i-1}, d)}{\gcd(r_{i-2}, d)}$.

I conclude: $d | r_i \& d | r_{i+1}$ for all $i > 0$.

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.

We know $d \mid N$ and $d \mid x$, and $d = y \cdot z + k \cdot N$.

The other way round: suppose $c \mid N$ and $c \mid x$.

Then $c \mid y \cdot z + k \cdot N = d$.

I.e. $d$ is a greatest common divisor.
\[ \mathbb{Z}_p \]

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/roots.

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

\[ \frac{p-1}{2} \neq \pm 1 \quad \text{then } p \text{ was }
\text{not prime!} \]

**Miller-Rabin - test**

\[ \text{Squarings} \quad \uparrow \]
\[ 1, \ldots, 1 \]
197

x

x, x^2, x^3, x^4, x^5, x^6, \ldots

197 196 \text{mult.}

13

x

x, x^2, x^4, x^8, x^{12}, x^{13}

197

197 = \frac{100000000}{n}

10 \text{ mult.}

\text{(instead of 12!)}

This needs at most

2(n-1) \text{ mult.}

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

The EEA computes

(a) the greatest common divisor $d$ of the input elements $x$ and $N$
(b) integers $s$ and $t$ such that

\[ d = s \cdot x + t \cdot N. \]

So either $g = 1$ (or $g = -1$) and $s x + t N = 1$ and $x^{-1} = s$ in $\mathbb{Z}_N$

or $g \neq \pm 1$

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

and no solution of $s x + t N = 1$

exists

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

\[ x \mod N \]

Corollary

unit group of $\mathbb{Z}_N$

\[ \mathbb{Z}_N^* := \{ x \in \mathbb{Z}_N \mid \exists y \in \mathbb{Z}_N : x y = 1 \text{ (in } \mathbb{Z}_N) \} \]

\[ = \{ [x] \in \mathbb{Z}_N \mid x \text{ is invertible} \}
\]

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

\[ \cup \{ [0] \} \]

Pf

Take $x \in \mathbb{Z}_N$ i.e. $\exists y \in \mathbb{Z}_N : x y = 1$.

Write $x = \frac{[x]}{e_2}$ and $y = \frac{[y]}{e_2}$

Now we know $[y] \cdot [x] + k \cdot N = 0$. for some $k \in \mathbb{Z}$.

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

Thus $x = \frac{[x]}{e_2} \mod N \in \mathbb{Z}_N$. 

Thus $x = \frac{[x]}{e_2} \mod N \in \mathbb{Z}_N$. 

\[ [x] \mod N \]
Take $x \in \mathbb{N}$, i.e. $x = 3x \equiv \text{mod } N$ 
with $7x \in \mathbb{Z}$, $0 \leq 3x \lt N$ 
and $\gcd (7x, N) = 1$.

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

$$1 = 7x \cdot t + x \cdot s$$

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

I.e. $x \in \mathbb{Z}_N$.

**Example**

$\mathbb{Z}_{15} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 \}$

$\mathbb{Z}_{15}^x = \{ 1, 2, 4, 7, 8, 11, 14 \}$

because $2 \cdot 8 = 16 \equiv 1 \pmod{15}$

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

$3 \in \mathbb{Z}_{15}^x$ because $\gcd (3, 15) = 1 + 3$.

*Side remark:* $1^2 = 1$, $(-1)^2 = 1$

and $4^2 = 1$, $(-4)^2 = 1$.

Thus $x^2 = 1$ has 4 solutions.

**Ex**

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

$12 = 2^2 \cdot 3$

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

\[ * \]
Question

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

Compute the sequence

\[ 1, x, x^2, x^3, x^4, \ldots \]

by multiplying \( x \) by itself to get a new element.

What special properties does the sequence have?

Ex

\[ N = 6, \ x = 2 \text{ in } \mathbb{Z}_6. \]

\[ \# \mathbb{Z}_N^x = 2 \]

\[ \text{period 2} \]

Observation: this sequence is periodical from some point.

\[ N = 15, \ x = 7 \text{ in } \mathbb{Z}_{15}. \]

\[ \# \mathbb{Z}_{15}^x = 8 \]

\[ \text{again: periodical!} \]

\[ N = 7, \ x = 2 \ldots \]

\[ \# \mathbb{Z}_7^x = 6 \]

\[ \text{period 3} \]

\[ N = 15, \ x = 5 \]

\[ \# \mathbb{Z}_{15}^x = 8 \]

\[ \text{period 4} \]
(i) The set of possible elements is finite.
(ii) The successor of an element is determined.

\[ \Rightarrow \text{These must be repetitions.} \]

Observe

If \( x \) is irreducible, so is any power \( x \) of \( x \).

In other words: if \( x \in \mathbb{Z}_N^x \) so is any \( x^k \in \mathbb{Z}_N^x \).

Thus the longest possible repetition length is \( \# \mathbb{Z}_N^x \) in case \( x \in \mathbb{Z}_N^x \).

Now:

\[ \# \mathbb{Z}_5^x = \# \{ 1, -1 \} = 2 \]
\[ \# \mathbb{Z}_6^x = \# \{ -1, 2, 4, 5, 7, 3 \} = 8 \]
\[ \# \mathbb{Z}_7^x = 7 - 1 = 6 \]

Lemma

If \( p \) is prime, then \( \# \mathbb{Z}_p^x = p - 1 \).
Observation

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

\[ G \text{ is a group: a set } G \text{ is finite such that axioms hold.} \]

Further, all our groups are finite.

Examples \(( \mathbb{Z}_n^X, \cdot) \) is a \( \text{comm.} \) group.

Let \( a, b \in \mathbb{Z}_n^X \), then \( a \cdot b \in \mathbb{Z}_n^X \).

- \( \cdot \) is \( \text{closed} \) in \( \mathbb{Z}_n^X \).
- \( \times \) is \( \text{associative} \).
- \( 1 \in \mathbb{Z}_n^X \) acts as \( \text{identity} \).
- \( a^{-1} \in \mathbb{Z}_n^X \) is \( \text{inverse} \) of \( a \).

(Examples \(( \mathbb{Z}_N, +) \) is also \( \text{comm.} \).)
Claim: This is also a list of all group elements. 

We prove this only for cyclic groups.

Let's note that if $x$ is a group element, then $x^i$ is also a group element for all integers $i$. 

For any group $G$, we can take any element $g_i$ of $G$ and form the product $g_i^k$, where $k$ is any integer. 

If $G$ is a finite group, then there are only finitely many possible values for $g_i^k$. Thus, we can write down a list of all group elements. 

In other words, if $G$ is a finite group, then the sequence $g_i, g_i^2, g_i^3, \ldots, g_i^n$ contains all elements of $G$. 

Therefore, we have shown that any finite group is cyclic.
So

\[
g_1 \cdots . g_s = x g_1 \cdot g_2 \cdots \cdot g_s
\]

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

Thus

\[
g_1 \cdots . g_s = x^s \cdot g_1 \cdots . g_s
\]

Multiply by \((g_1 \cdots . g_s)^{-1}\):

\[
x = x^s
\]

This is what we wanted since \(s = \#G\).

\[
\text{Corollary (Euler)}
\]

Suppose \(N > 2\) and \(x \in \mathbb{Z}_N^x\). Then

\[
x \equiv (N) \equiv 1 \pmod{\mathbb{Z}_N}
\]

where \(\phi(N) \equiv \#\mathbb{Z}_N^x\).

Euler totient function.

\[
\text{Corollary (Little Fermat Theorem)}
\]

Suppose \(p\) is prime and \(x \in \mathbb{Z}_p^x\). Then

\[
x^{p-1} \equiv 1 \pmod{\mathbb{Z}_p}
\]

If apply Euler's theorem with \(N = p\) and observe \(\phi(p) = p - 1\).
Corollary 3.27

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

Then \( x^p = x \) (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. \( \square \)

---

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: \( \phi(N) = \# \mathbb{Z}_N^\times = L \).

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 \( \# \mathbb{Z}_{p \cdot q}^\times = (p-1)(q-1) \)?

The \( gcd(x, p \cdot q) \) could be

1, \( p \), \( q \) or \( p \cdot q \),

and nothing else.
\[ a, 1, 2, 3, \ldots \text{ do not exist} \]

9-1 elements have \( \gcd(x, pq) = p \)

\[ \begin{aligned}
\text{p-1} & = 9 \\
\text{1} & \quad \text{gcd}(x, pq) = p \cdot q \\
\end{aligned} \]

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

Thus there are \( pq - q + 1 - p + 1 - 1 \) invertible elements.

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

\[ \text{ie.} \quad \phi(N) = \frac{N}{\phi(N)} \]
Towards the Chinese Remainder Theorem

Teacher puts pupils in rows of 2
\[ \Rightarrow 1 \text{ pupil remains.} \]
Teacher puts pupils in rows of 3
\[ \Rightarrow 1 \text{ pupil remains.} \]
Teacher puts pupils in rows of 5
\[ \Rightarrow 3 \text{ remain.} \]
How many pupils were there?

Rephrase that: Find the number \( x \)
such that
\[ x \equiv 1 \pmod{2}, \]
\[ x \equiv 1 \pmod{3}, \]
\[ x \equiv 3 \pmod{5}. \]

The answer is \( x = 13 \) or \( x = 43 = 13 \times 3 + 2 \times 5 \)

or \( x = 73 \) or...

For short: \( x \equiv 13 \pmod{30}. \)
Chinese Remainder Theorem

Suppose \( N = N_1 N_2 \) with \( \gcd(N_1, N_2) = 1 \). Then the map

\[
\mathbb{Z}_N \rightarrow \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}
\]

\[
x \mod N \mapsto (x \mod N_1, x \mod N_2)
\]

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

**Example**

\[
\begin{align*}
\mathbb{Z}_{15} & \quad \mathbb{Z}_3 & \quad \mathbb{Z}_5 \\
\text{elements} & \quad \text{elements} & \quad \text{elements} \\
\mod 15 & \quad \mod 3 & \quad \mod 5 \\
x \times x & \quad x + 15
\end{align*}
\]

**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

\[
x \equiv a_1 \mod N_1 \text{ and } x \equiv a_2 \mod N_2.
\]
Consider $N=15$, $x=7$ in $\mathbb{Z}_{15}$.

We had the sequence:

\[ \mathbb{Z}_3 : \begin{align*} 1 & \mapsto 1 \\ 7 & \mapsto 4 \\ 4 & \mapsto 1 \\ -2 & \mapsto 4 \end{align*} \]

\[ \mathbb{Z}_5 : \begin{align*} 1 & \mapsto 1 \\ 7 & \mapsto 4 \\ -2 & \mapsto 4 \end{align*} \]

Reduce:

\[ \mathbb{Z}_3 : \begin{align*} 1 & \mapsto 1 \\ 1 & \mapsto 1 \\ 1 & \mapsto 1 \\ 1 & \mapsto 1 \end{align*} \]

\[ \mathbb{Z}_5 : \begin{align*} 1 & \mapsto 1 \\ 2 & \mapsto -1 \\ -2 & \mapsto 1 \end{align*} \]

The reduction of 7 is $7 \mod 3 = 1$.

So, it is the same whether we think in $\mathbb{Z}_{15}$, or in $\mathbb{Z}_3 \times \mathbb{Z}_5$.

**Example:**

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

\[ \begin{align*} \mathbb{Z}_N : & \quad 1, 4, -5, 1, \ldots \\ \mathbb{Z}_3 \times \mathbb{Z}_7 : & \quad 1, 4, -5, 1, \ldots \end{align*} \]

$4 \equiv (4 \mod 3, 4 \mod 7) \equiv (1, -3)$

\[ \begin{align*} 1 & \mapsto 1 \\ 4 & \mapsto 1 \\ -5 & \mapsto 1 \\ 1 & \mapsto 1 \end{align*} \]
$\mathbb{Z}_6 : \{0, 1, 2, 3, 4, 5\}

$\mathbb{Z}_2 \times \mathbb{Z}_3 : \{0, 1, 2, 0, 1, 2\}

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

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

Pairs:
- $(0, 0)$, $(0, 1)$, $(0, 2)$,
- $(1, 0)$, $(1, 1)$, $(1, 2)$

$3 + 4 \equiv (1, 0) + (0, 1)$

$= (1 + 0, 0 + 1)$

$= (1, 1) \equiv 1$

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.
$3 \mod 14$

$3^{100} \text{ in } \mathbb{Z}_{1001}$

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

$3^0 = 9$
$3^1 = 27$
$3^2 = 729$
$3^3 = 531 \cdot 441$
$\quad = 531 \cdot 1000 + 441$
$\quad = 531 + 441$
$\quad = 90$

$3^{100} = (90)^{100}$
$3^{100} = \left(\frac{531 \cdot 441}{531}\right)^{100} \cdot 5$

Division with remainder

$\begin{cases} a, b \in \mathbb{Z}, b > 0 \\ a = q \cdot b + r, \quad 0 \leq r < b \end{cases}$

What is a polynomial?

It is linear combination of powers of some variable(s).

Ex. $\frac{5x^2 + 1x - 2}{2} \in \mathbb{Z}$ is a polynomial "over $\mathbb{Z}$."
\[ n^3 + 2n \in O(n^3) \]

degree = 3

\[ \frac{S x^2 + 1x - 2}{\mathbb{Z}_n, \mathbb{Z}_n, \mathbb{Z}_n} \text{ over } \mathbb{Z}_n \]

\[(Sx^2 + x - 2)^2 \]
\[= (Sx^2 + x - 2) \cdot (Sx^2 + x - 2) \]
\[= Sx^2 (\underline{\overline{Sx^2}}) + x (\underline{\overline{Sx^2}}) - 2(\underline{\overline{Sx^2}}) \]
\[= (S \cdot S)x^4 + (S \cdot 1 + 1 \cdot S)x^3 \]
\[+ (S \cdot (-2) + 1 \cdot 1 + (-2) \cdot S)x^2 \]
\[+ (1 \cdot (-2) + (-2) \cdot 1) x + (-2) \cdot (-2) \]
\[= 3x^4 - 1x^3 + 3x^2 - 4x + 4 \]

\[ \mathbb{Z}_2 = \{0, 1\} \]

\[ \mathbb{Z}[x] \ni x^3 + x + 1 = \frac{x^3 + 1}{(x + 1)(x^2 + 1)} \]

division with remainder for polynomials over a field

\[ a, b \in F[x], \ b \neq 0 \]

field for coefficients, the variable

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

\[ \deg(r) = -\infty. \]
way to do this:
write \( P \) by coordinates
find a formula for the coordinates of \( R \).

To get a finite group:
use coefficients/numbers
but from \( \mathbb{Z}_p \) for one prime.

This formula depends highly on the representation of the points \( P, Q \).
Probability

- error detection
- input distribution + reaction test & randomized algorithms
- gambling: winning probability, expected win

Le coin tossing

Monty Hall Problem

Choose one
host opens another with goat.
do you switch?
Factoring

Pollard-g

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

Solution proposed

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

Compute $x_0, x_1 = f(x_0), \quad x_2 = f(x_1), \quad x_3 = f(x_2),$
until two of them coincide modulo $p$!

We can detect that without knowing $p$ by computing
$p : \gcd(x_i - x_j, N) \neq 1$

$N / p$

Input: $N$.
Output: Either a factor $p$ or FAIL.

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

Heuristically, expected time $\sqrt[3]{N}$.
Consider a program with a loop

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

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

How many iterations of the loop do you expect?

More concrete

1. repeat
2. \( n \in \mathbb{N}, n \leq 42 \)
3. until \( n = 0 \).

What is the average running time? (expected)

42!
Send me an email to
nuesken@bit.uni-bonn.de

finite probability space
U finite set

\[ \mathbb{P}: U \to [0,1] \]

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

Example coin tossing: "fair coin"

\[ U = \{ \text{heads, tails} \} \]

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

coin tossing including "nim"

\[ U = \{ \text{heads, nim, tails} \} \]

\[ \mathbb{P}(\text{heads}) = 0.499, \quad \mathbb{P}(\text{tails}) = 0.499, \quad \mathbb{P}(\text{nim}) = 0.002 \]

1 die
rolling a three sided die
\[ U = \{ \cdot , \cdot , \cdot , \cdot \} \]

\[ \mathbb{P}(\cdot ) = \frac{1}{3}, \quad \mathbb{P}(\cdot \cdot ) = \frac{1}{3}, \quad \mathbb{P}(\cdot \cdot \cdot ) = \frac{1}{3} \]

2 dice
rolling a "special" die
\[ U = d \cdot , \cdot , \cdot , \cdot \]

\[ \mathbb{P}(\cdot ) = \frac{1}{6}, \quad \mathbb{P}(\cdot \cdot ) = \frac{1}{6}, \quad \mathbb{P}(\cdot \cdot \cdot ) = \frac{1}{6} \]
Fair die:
\[ U = \{1, 2, 3, 4, 5, 6\} \]
\[ P(i) = \frac{1}{6} \text{ for each } i \in U. \]
\[ \text{prob(roll an even number)} = \]
\[ = P(2) + P(4) + P(6) = \frac{1}{2}. \]

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

An event is a subset of \( \Omega \).

We define \( \text{prob}(A) = \Sigma_{x \in A} P(x) \).

Now obviously we have:

- null event \( \emptyset = \{\} \): \( \text{prob}(\emptyset) = 0 \)
- \( \Omega \): \( \text{prob}(\Omega) = 1 \).
- 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 \( A, B \subseteq \Omega \).
  \[ \text{prob}(A \cap B) = \text{prob}(A) + \text{prob}(B) - \text{prob}(A \cup B) \]
\[ \text{2} \cdot \text{prob}(A \cap B) \leq \text{prob}(A) \cdot \text{prob}(B) \]

Ex. Fair die:

\[ A = \{2, 4, 6\}, \quad B = \{4, 5, 6\} \]

\[ \text{prob} \ A = \frac{1}{2} \]

\[ \text{prob} \ B = \frac{1}{2} \]

\[ \text{prob} (A \cap B) = \text{prob} \{4, 6\} = \frac{1}{3} \neq \frac{1}{2} \cdot \frac{1}{2} \]

\[ \text{\textbf{A} and B are not independent} \]

Define: Two events A and B are called independent iff

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

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

Conditional probability of A given B

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

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

\[ (B, u \rightarrow \text{prob}(E \cup 31 | B)) \]
Ex

Fair die

\[ A = \{2, 4, 8\} \]
\[ B = \{1, 2\} \]
\[ \text{prob}(A) = \frac{1}{3} \]
\[ \text{prob}(B) = \frac{1}{3} \]
\[ \frac{\text{prob}(A \cap B)}{\text{prob}(B)} = \frac{\frac{1}{3}}{\frac{1}{3}} = 1 \]

Now \( A \) and \( B \) are independent

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

Ex

Rusty Hall example

\[ U = \{1, 2, 3\} \]
\[ P(4) = \frac{1}{3} \] for any \( u \in U \)

\[ B = \{1, 2\} \]
\[ \text{prob}(1 \mid B) = \frac{\text{prob}(1)}{\text{prob}(B)} = \frac{\frac{1}{3}}{\frac{1}{3}} = 1 \]
\[ \text{prob}(2 \mid B) = \frac{1}{2} \]

\[ \boxed{\text{This does not describe the show.}} \]

Right answer:

\[ \text{prob( car with switch) = prob( one door) = } \frac{1}{3} \]
\[ \text{prob( car with switch) = prob( two doors) = } \frac{2}{3} \]
A real random variable $X : U \rightarrow \mathbb{R}$, with

\[
e_{\text{ex}} X = \text{running time of the program } \text{of the program}
\]

1. repeat
2. $x \in \mathbb{R}$
3. $u \sim \mathcal{L}(x = 0)$

**Expected value of $X$**

\[
E(X) = \sum_{u \in U} X(u) P(u) \\
= \sum_{x \in X(U)} x \cdot \text{prob}(X = x)
\]

\[
\sum_{x \in X(U)} x \cdot \text{prob}(X = x)
\]

<table>
<thead>
<tr>
<th>$u$</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X(u)$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$X(u)$</td>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{6}$</td>
</tr>
</tbody>
</table>

**Ex.** Fair die, $X(u) = u$.

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

\[
= \frac{21}{6} = 3.5.
\]

**Variance**

\[
\text{var}(X) = E((X - E(X))^2)
\]

**Standard deviation**

\[
\text{stddev}(X) = \sqrt{\text{var}(X)}
\]
Suppose $X, Y$ random variables (over the same universe)

\[ X, Y \text{ independent } \iff \]

\[ \Pr(X = x, Y = y) = \Pr(X = x) \cdot \Pr(Y = y) \]

for all possible $x, y$.

Again:

\[ \Pr(X = x \mid Y = y) = \Pr(X = x) \]

(provided $\Pr(Y = y) \neq 0$).

Consider a program of the form

\[
\text{repeat}
\begin{align*}
\text{body} \\
\text{until } X_i = 1
\end{align*}
\]

What is the expected running time if $\Pr(X_i = 1) = p$ for all indices $i$, and the r.v. $X_i$ are p.r. independent?\[ \Pr(X_i = 0) = 1 - p \approx 0.6. \]

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

\[
Y^{(n)} \begin{cases} 
= i & \text{if } X_1 = 0, X_2 = 0, \ldots, X_i = 0 \\
= n+1 & \text{if } X_1 = \ldots = X_n = 0 
\end{cases}
\]

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

Calculate

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

Now, in case $i \leq n$,

\[
\text{prob}(Y^{(n)} = i) = \text{prob}(X_1 = 0, X_2 = 0, \ldots, X_i = 0, X_{i+1} = 1) = \prod_{j=1}^{i} \text{prob}(X_j = 0) \cdot \prod_{j=i+1}^{n} \text{prob}(X_j = 1)
\]

and

\[
\text{prob}(Y^{(n)} = n+1) = 6^n
\]

Thus

\[
E(Y^{(n)}) = \sum_{i=1}^{n} i \cdot 6^{-i} + (n+1)6^n
\]
We know
\[ \sum_{i=0}^{n} \delta_i = \frac{1 - \delta^{n+1}}{1 - \delta}. \]

\[ \sum (1 - \delta) \cdot \sum \delta_i = 1 + \delta + \ldots + \delta^n - \delta - \ldots - \delta^n - \delta^{n+1} \]

Derive this m.r.t. \( \delta \):
\[ \sum_{i=0}^{n} \delta^{i-1} = \frac{(1 - \delta^{n+1}) (1 - (n+1) \delta (1 - \delta))}{(1 - \delta)^2} \]

\[ = \frac{-1 + \delta^n - (n+1) \delta^2 + (n+1) \delta^{n+1}}{(1 - \delta)^2} \]

\[ = -1 - (n+1) \delta^n + (n+1) \delta^{n+1} \]

\[ \frac{-n \delta^n + \frac{1 - \delta^n}{(1 - \delta)^2}}{1 - \delta} \]

Back to our calculation
\[ E(Y^{(m)}) = \sum_{i=0}^{n} \delta^{i-1} \cdot \delta + (n+1) \delta^n \]

\[ = -n \delta^n + \frac{1 - \delta^n}{1 - \delta} + (n+1) \delta^n \]

\[ = \frac{1 - \delta^n}{1 - \delta} + \delta^n \]

\[ = \frac{1}{\delta} + \delta^n \left( 1 - \frac{1}{\delta} \right) \]

We let \( n \to \infty \):

\[ \lim_{n \to \infty} E(Y^{(m)}) = \frac{1}{\delta}. \]
Theorem

The expected running time of a loop which terminates independently after an iteration with probability \( p > 0 \) is equal to \( \frac{1}{p} \).
(a) What is the probability space (and distribution) for Roulette?

There are 38 small "baskets" named 0, 00, 1, 2, ..., 36.

You can bet:
(a) on a single number
   payoff 36 x amount
(b) on halves: 1 odd / 18 even, 1 high / 18 low, 1 red / 18 black
   payoff 2 x 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 quarte.

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

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 conditional probability that the sum of the dice is even given none shows a six.

Ex 2.3 Give an example where an average winning line is 60.
Streaming application

bit

100MBit/s

100MBit/s

How to transmit?

\( f = 100 \text{ MBit/s} \)

\( f_1 = 100 \text{ MBit/s} \)

\( f_2 = 10 \text{ MBit/s} \)

\( F = 1 \text{ sec} \)

\( f_1 = 100 \text{ MBit/s} \)

\( f_2 = 10 \text{ MBit/s} \)

\( t_1 = 1 \text{ sec} \)

\( t_2 = 10 \text{ sec} \)

\( t = 5.5 \text{ sec} \)

Same time constraint: same time for any part of data (to avoid buffering!)
Conditions

\[ T = t_1 + t_2 \]

\[ T = t_3 \]

\[ f_1 = \text{100 Mbps/sec} \cdot t_1 \]

\[ f_2 = \text{10 Mbps/sec} \cdot t_2 \]

\[ f_3 = \text{10 Mbps/sec} \cdot t_3 \]

From now on we drop units "Mbps" and "sec".

\[ f_1 = f_2 \]

\[ f_1 + f_3 = f \]

\[ f_2 + f_3 = f \]

Number of equations = 8
Number of unknowns = 8 including \( f, T \)

If we consider \( f \) given.

Actually the equations (A), (B), and (C) are dependent, we can drop one of them without losing information.

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

\[ (A') \quad 100 t_1 = 10 t_2 \]

\[ (B') \quad 100 t_1 + 10 t_3 = f \]

\[ (C') \quad 10 t_2 + 10 t_3 = f \]

\[ (\alpha') \quad T = t_1 + t_2 \]

\[ (\beta') \quad T = t_3 \]
Now we have essentially 4 eq. and 4 var.

<table>
<thead>
<tr>
<th></th>
<th>t₁</th>
<th>t₂</th>
<th>t₃</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A')</td>
<td>100</td>
<td>-10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(b')</td>
<td>100</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>v (pc')</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>v (a')</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>v (b')</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Gauß elimination
\[ t₁ \]

Gauß-Jordan algorithm
\[ t₂ \]

Allowed elementary operations:

1. Exchange rows
2. Multiply a row by a invertible number
3. Subtract/add a multiple of a row from/to another row.

This is the Gauß-Jordan algorithm.
\( t_1 = \frac{f}{210} \)
\( t_2 = 10 \frac{f}{210} \)
\( t_3 = 11 \frac{f}{210} \)
\( T = 11 \frac{f}{210} \)

\( f = 210\ \text{MBit} \)

Constraints:
- Given: a network including bandwidth, source and destination.
- 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 \( f_i = t_i \cdot \text{bandwidth of the edge} \).
In adjacency matrices:

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

$$A_{uv} = 1 \text{ if } \exists e \in E: e \text{ is an edge from } u \text{ to } v.$$  

Concrete graph:

$$1 \rightarrow 2 \rightarrow 3 \rightarrow 4$$

$$A = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1
\end{pmatrix}.$$  

Matrix multiplication:

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

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

$$C = A \cdot B$$

$$C_{wu} = \sum_v A_{uv} B_{vu}$$
Matrix multiplication can help us to count paths in graphs.

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

\[
(A^2)_{uw} = \sum_v A_{uv} A_{vw}
\]

*edges \( u \to v \)  
*edges \( v \to w \)

\# 2-paths \( u \to v \to w \)

\# 2-paths \( u \to w \)

In the example:

\[
A^3 = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

\( A^3 \) counts paths of length 3

Line: \( A^3 = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix} \)

\( I + A + A^2 + \ldots + A^{n-1} \) counts all paths of length \( \leq n \).

Suppose \( G \) has no cycles: then \( n = \#V \)
By computing \( I + A + A^2 + \ldots + A^{n-1} \)
we can isolate the connected components.

If we replace addition with the \( m \)-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:
\[
I + A + \ldots + A^{n-1} = (I - A^n) (I - A)^{-1}.
\]

\text{Pf.}
\[
(I - A) \cdot (I + A + \ldots + A^{n-1})
= I + A + \ldots + A^{n-1}
- A - \ldots - A^{n-1} - A^n = I - A^n.
\]

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

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 \( 25 \times 25 \)
There cannot be an algo. with less than \( 2n^2 - 1 \) ops'
Do you think one can multiply matrices with $O(n^{2.8})$ ops?

or $O(n^{2.38})$ ops?

or $O(n^{2.37})$ ops?

Yes! Strassen 1971

Gaussian elimination is not optimal.

UNKNOWN

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 ops can be transformed to matrix multiplication with "simple" matrices:

- exchange rows $i,j$
  $$P_{ij}$$
  $$P_{ij}A \cdot x = P_{ij}b$$

- multiply a row $i$ with an invertible number $t$
  $$S_{it}A \cdot x = S_{it}b$$
Als ersten Schritt zerlegen wir die Matrizen $A, B$ und $C = A \cdot B$ in Blöcke der Größe $\frac{n}{2}$
\[
\begin{pmatrix}
C_{11} & C_{12} \\
C_{21} & C_{22}
\end{pmatrix} = 
\begin{pmatrix}
A_{11} & A_{12} \\
A_{21} & A_{22}
\end{pmatrix} \cdot 
\begin{pmatrix}
B_{11} & B_{12} \\
B_{21} & B_{22}
\end{pmatrix}
\]

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

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

\[
T(n) \in 7T\left(\frac{n}{2}\right) + O\left(n^2\right)
\]
\[T(n) = 7T\left(\frac{n}{2}\right) + 18n^2,\quad T(1) = 1.
\]

Let's ignore additions:
\[T(n) = 7T\left(\frac{n}{2}\right)\]
\[T(1) = 1.
\]

Heuristics: \[T(n) = 7 \cdot T\left(\frac{n}{2}\right) = 7 \cdot 7 \cdot T\left(\frac{n}{4}\right) = 7^3 T\left(\frac{n}{4}\right)
\]

Suppose $n = 2^k$ then $T(n) = 7^k \cdot T\left(\frac{n}{2^k}\right) = 7^k
\]
\[k = \log_2 n \quad \Rightarrow \quad T(n) = 7 \cdot \log_2 n = (2 \cdot \log_2 7) \cdot \log_2 n
\]
\[= (2 \cdot \log_2 7)^{\log_2 n} = n^{\log_2 7} \approx 2.80... \times 2.81. \text{ thus } O(n^{2.81})\]
Suppose \( A \) is any matrix of format \( m \times n \).
There is a sequence of elementary operations such that the resulting matrix
is of the form

\[
\tilde{A} = \begin{pmatrix}
\text{1} & * & * & \cdots & * \\
\text{0} & \text{1} & * & \cdots & * \\
\vdots & \vdots & \ddots & \cdots & \vdots \\
\text{0} & \text{0} & \cdots & \text{1} & * \\
\end{pmatrix}
\]

and this process can be written as

\[
\tilde{A} = \mathbf{T}_n \cdots \mathbf{T}_2 \mathbf{T}_1 A
\]

where each \( \mathbf{T}_i \) is one of the elementary matrices and if we do not insist on \( * = 0 \),
each of them is lower triangular apart from the permutation (row swaps). But
these can be done in advance so we have

\[
\pi(\tilde{A}) = \begin{pmatrix}
\text{1} & * & * & \cdots & * \\
\text{0} & \text{1} & * & \cdots & * \\
\vdots & \vdots & \ddots & \cdots & \vdots \\
\text{0} & \text{0} & \cdots & \text{1} & * \\
\end{pmatrix}
\]

where \( \pi \) is lower triangular and \( P \) is a permutation.
Then being careful we obtain
\[ P \cdot A = LU \]
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
\[ PAX = Pb \]
\[ LUX = Y \]
in two steps:
\[ L \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \end{bmatrix} = Pb \]
\[ UX = Y \]
Let's do this:

\[
\begin{pmatrix}
1 & 6 & 8 \\
3 & 5 & 3 \\
12 & 2 & 10
\end{pmatrix}
\begin{pmatrix}
4 & 1 & 0 \\
0 & 1 & 0 \\
1 & 0 & 1
\end{pmatrix}
\quad \text{\{mod 15 over } \mathbb{Z}_{13}\}\]

\[
\begin{pmatrix}
1 & 6 & 8 \\
0 & 0 & 2 \\
0 & 0 & 5
\end{pmatrix}
\begin{pmatrix}
4 & 1 & 0 \\
1 & -3 & 1 \\
5 & 10 & 1
\end{pmatrix}
\]

\[
\begin{pmatrix}
1 & 6 & 8 \\
0 & 1 & -1 \\
0 & 0 & 2
\end{pmatrix}
\begin{pmatrix}
4 & 1 & 0 \\
-1 & 5 & 0 \\
-1 & 3 & 10
\end{pmatrix}
\]

\[
\begin{pmatrix}
1 & 6 & 8 \\
0 & 1 & -1 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
4 & 1 & 0 \\
-1 & 5 & 0 \\
7 & 0 & 1
\end{pmatrix}
\]

\[
\begin{pmatrix}
4 & 1 & 0 \\
5 & 0 & 5 \\
5 & 0 & 5
\end{pmatrix}
\]

\[
\begin{pmatrix}
1 & 6 & 8 \\
0 & 1 & -1 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 \\
5 & 0 & 5 \\
5 & 0 & 5
\end{pmatrix}
\]

\[
\begin{pmatrix}
1 \rightarrow 1\cdot \mathbf{P} \\
0 \rightarrow \mathbf{L} \cdot \mathbf{P} \\
0 \rightarrow \mathbf{L}
\end{pmatrix}
\]

\[
\mathbf{P} = \begin{pmatrix} 1 & 0 & 1 \\ -5 & 7 & 5 \end{pmatrix}, \quad \mathbf{L} = \begin{pmatrix} 1 & 0 & 1 \\ -5 & 7 & 5 \end{pmatrix}
\]

Thus

\[
\mathbf{A} = \mathbf{P}^{-1} \mathbf{L} \mathbf{U}
\]
or

\[
\mathbf{P} \mathbf{A} = \mathbf{L} \mathbf{U}
\]

\[
\det \mathbf{A} = 10, \quad \det \mathbf{P} = -1, \quad \det \mathbf{L} = (\det \mathbf{L}^T)^{-1} = (-1)^{-1} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]

\[
\det \mathbf{U} = 1
\]
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 solutions?

Concerning (i):
To find all solutions of $Ax = b$, we have to find
- find one solution $x_0$ of $Ax = b$,
- all solutions $S_x$ of the homogeneous equation $Ax = 0$.

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

$0 \in S_A$, ($\lambda$ a number, $x \in S_A \Rightarrow \lambda x \in S_A$), $S_A$ is a vector space over the field?
no solution because last line says:
\[ 0 \cdot x_3 = 3/2. \]
\[ \Rightarrow \text{dim 1 many solutions} \]
(over \( Z_{13} \): 15!)

\[ \Rightarrow \text{dim. 2 many solutions} \]
(over \( Z_{13} \): 13²)

\[ (Z_{13} \times Z_{13}) \]
\[ (0,0) \quad (0,1) \ldots \quad (12,12) \]
\[ (1,0) \quad (1,1) \ldots \]
\[ \vdots \]
\[ \vdots \]
\[ (12,12) \]

Determinants

\[ \det I = 1 \]
\[ \det (A \cdot B) = \det A \cdot \det B \]
\[ \text{if } P \text{ swaps rows} \]
\[ \det (PA) = -\det A \]
\[ \det (AP) = -\det A \]
\[ \det (S_{t \cdot A}) = t \cdot \det A \]
\[ \det (E_{t \cdot A}) = \det A \]
Fact

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

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

Ex 3.1 Solve the system of equations

\[
\begin{pmatrix}
1 & 0 & 3 \\
0 & 2 & 1 \\
1 & 0 & 0
\end{pmatrix}
\cdot x = \begin{pmatrix} 3 \\ -1 \\ 2 \end{pmatrix}
\text{ over } \mathbb{Z}_3.
\]

and calculate the determinant of the matrix.
Birthday problem

\[ \text{prob (two birthdays within } n \text{ persons coincide)} \]

\[ = 1 - \text{prob (within } n \text{ randomly chosen persons all have different birthdays)} \]

\[ = 1 - \left( \frac{365}{365} \right) \left( \frac{364}{365} \right) \left( \frac{363}{365} \right) \ldots \left( \frac{365-n+1}{365} \right) \]

\[ = 1 - \frac{\frac{\binom{365}{n}}{365^n}}{365} \approx \text{small!} \]

\[ 1 - s = \frac{n(n-1)}{2 \times 365} - \frac{n}{365^2} \approx c \cdot n^2 \]

Thus the expected number of persons until two have the same birthday will be about \( c \sqrt[3]{365} \).
Actually, we consider the following experiment:

1. repeat
2. choose a person \( p_i \) with a random birthday
3. until \((\text{two of the persons } p_j, \ldots, p_i \text{ have the same birthday})\)

Here, \( \text{prob ( stopping after person } i \text{ if all previous persons have diff. birthdays) } = \frac{i - 1}{365} \).

\[ Y \sim \text{r.v. giving the number of persons until two have same birth}\]

Thus \[ Y = n \text{ iff } X_n \in \{ X_1, \ldots, X_{n-1} \} \]

\[ \# \{ X_1, \ldots, X_{n-1} \} = n - 1 \]

So, the \( X_1, \ldots, X_n \) are pairwise different.

Of course:

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

\( \text{same day in the year} \)

The r.v. \( X_1, \ldots, X_{366} \) are (pairwise) independent.

\( \text{hypotheses} \) (\( = \text{modeling the situation} \))
We want to calculate (or estimate) the expected running time.

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

So

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

Now

\[ \text{prob}(Y=n) = \text{prob}(X_n \in d X_1, \ldots, X_{n-1}, \text{and } X_1, \ldots, X_n \text{ p.w. diff}) \]

and \( \square \) are not independent!

Ex. \( n = 3 \): \( \square \) is true, then

\[ \text{prob}(\square | \square) = \frac{2}{365} \]

but if \( \square \) is false then

\[ \text{prob}(\square | \neg \square) = \frac{1}{365} \]

So \( \square \) depends on \( \square \).

Recall

\[ \text{prob}(A \cap B) = \frac{\text{prob}(A \cap B)}{\text{prob}(B)} \]

and this rewriting gives

\[ \text{prob}(A \cap B) = \text{prob}(A | B) \cdot \text{prob}(B). \]
\[ \text{prob}(Y = \text{n}) = \text{prob}(\square 1 \square) \cdot \text{prob}(\square) \]

We know
\[ \text{prob}(\square 1 \square) = \frac{n \cdot 1}{365} \]

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

so putting this together yields

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

shows a "little maths manipulation" gives
\[ E(Y) \leq c \cdot \sqrt{365} \]
11-element addition chain for \( 382 = 1011100 \).

More info on that:
D.E. Knuth
The art of computer programming

\[
\frac{3}{2} = 3.4 = -2 = 5
\]

In calculations only \(-6, \ldots, 6\),
(letters: \(-3 \ldots 3\) or \(0 \ldots 6\)).

\[-2 = 5\]
\[2^{-1} = 4 = -3\] in \(\mathbb{Z}_7\).
Invertible polynomials in \( \mathbb{F}_2[x] \)

\[
(x^3 + x + 1) \quad \text{mod} \quad \frac{x^3 + x^2 + 1}{x^3 + 1}
\]

we look for a polynomial \( B \) such that

\[
(B \cdot A) \quad \text{rem} \quad M = 1
\]

i.e.,

\[
B \cdot A + K \cdot M = 1
\]

for some polynomial \( K \).

**EEA**

<table>
<thead>
<tr>
<th>( r_i )</th>
<th>( s_i )</th>
<th>( t_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x^3 + x^2 + 1 )</td>
<td>( x^4 + x^2 + x + 1 )</td>
<td>( 0 )</td>
</tr>
<tr>
<td>( x^3 + x + 1 )</td>
<td>( x \cdot x^3 + x^2 + x + 1 )</td>
<td>( 1 )</td>
</tr>
<tr>
<td>( x^2 + 1 )</td>
<td>( x \cdot x + 1 )</td>
<td>( x \cdot x^3 + x^2 + x + 1 )</td>
</tr>
<tr>
<td>( 1 )</td>
<td>( x )</td>
<td>( x^2 + 1 )</td>
</tr>
<tr>
<td>( 0 )</td>
<td>( x^3 + x^2 + 1 )</td>
<td>( x^5 + x + 1 )</td>
</tr>
</tbody>
</table>

\( \text{verified!} \)

**Result:**

\[
A = (x^2) \cdot (x^6 + x^5 + x^2 + x) \cdot A
+ (x^2 + x + 1) \cdot M
\]

Hence \( A \mod M = x^6 + x^5 + x^2 + x \).
Solving linear equations

Let's calculate over \( \mathbb{Z}_3 \).

**Problem**

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

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

(Original question: How many invertible 3x3-matrices are there over \( \mathbb{Z}_3 \)?)

To find a matrix \( X \) such that \( A \cdot X = I \).

(In other words: Find \( x_1, x_2, x_3 \) vectors such that \( A \cdot x_1 = (0), A \cdot x_2 = (0), A \cdot x_3 = (0) \).)
\[ \begin{align*}
1:31.6 \\
-3 & 1 \\
2 & 4 \\
0 & 7 \\
\end{align*} \]

\[ \begin{align*}
1:32.5 \\
1 & 6 \\
2 & 4 \\
0 & 7 \\
\end{align*} \]

\[ \begin{align*}
1:33.6 \\
1 & 4 \\
2 & 3 \\
0 & 7 \\
\end{align*} \]

\[ \begin{align*}
1:34.6 \\
1 & 0 \\
0 & 5 \\
0 & 7 \\
\end{align*} \]

\[ \begin{align*}
1:35.6 \\
1 & 0 \\
0 & 0 \\
0 & 8 \\
\end{align*} \]

\[ \begin{align*}
1:36.6 \\
1 & 0 \\
0 & 0 \\
0 & 9 \\
\end{align*} \]

\[ \begin{align*}
1 & 0 \\
0 & -5 \\
0 & 6 \\
0 & 3 \\
\end{align*} \]

\[ \begin{align*}
1 & 0 \\
0 & 6 \\
0 & 4 \\
\end{align*} \]

So! \( A \) is invertible,

\[
\begin{pmatrix} -3 & -7 & -1 \\ 6 & 8 & 1 \\ 9 & 4 & 4 \end{pmatrix}
\]

\[
\begin{pmatrix} -3 \\ -7 \\ 5 \end{pmatrix} \]

\[
\begin{pmatrix} -3 & -7 & -1 \\ 6 & 8 & 1 \\ 9 & 4 & 4 \end{pmatrix}
\]

Another way for determinant \( \det \):

Suppose \( \det \): lower triangular, upper triangular

Then \( \det A = \det L \cdot \det U \)

\[
\begin{pmatrix} 1 & 1 & 1 \\ 2 & -9 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}
\]

\[ \text{cubic! time!} \]

\[ \text{no swaps.} \]

\[ \text{for determinant} \]

\[ \text{def } \]