
Informaatika Piirid

Margus Niitsoo



Miks mina siin olen?

- Põhiala Krüptoloogia
 - Sellest see aasta ei räägi...
- AGA
 - Krüpto on piiridega seotud
 - Filosoofilised huvid



Loengu tagasiside

Kirjutage:

- Mida uut saite teada?
- Mida juba teadsite?
- Muud kommentaarid



Alustame algusest

- Mida tähendab “kolm”?
- Mis juhtub, kui meil numbreid ei ole?
- “rohkem”, “vähem”?



Huvitava osa juurde

- Mängime mängu nimega “Hilberti hotell”
- Olete hotelli administraator
 - Lõpmatu hotell
 - Ja see on täis!



Keskkool

- Erinevad arvude tüübid:
 - Naturaalarvud
 - Täisarvud
 - Ratsionaalarvud
 - Reaalarvud



Matemaatiliselt rääkides

- Täisarve on sama palju kui naturaalarve
- Ratsionaalarve on ka sama palju
- Nojah - lõpmatult..



Interesting Twist

- Reaalarve on rohkem!
 - Georg Cantor ~1900
- Tõestus..



Vaheküsimus:

- Kui palju on erinevaid võimalikke arvutiprogramme?
- Kas leidub midagi, mida on vähem, kui reaalarve, aga rohkem kui naturaalarve?



Ja edasi?

- Ok, see oli matemaatika
- Mis sel arvutitega pistmist on?



Vahetame teemat

- Kas järgnev programm lõpetab alati töö?

```
arv=input()  
while (arv<=0) :  
    arv=-arv  
return arv*arv*arv
```



Küsimus

- Kas te oskaks kirjutada programmi, mis seda kontrollib?
- Kui ise ei oska, siis kas see on teie arvates võimalik?



Turing, 1936

EI OLE!



Tõestus

- Eeldame vastuväiteliselt et on
 - St, leidub alati töötav programm “**FIN(prog, sisend)**”
 - Eeldame et nii programm kui sisend on **baitkoodis**
 - St – nad on **arvud**
 - Tabel!



Tõestus a la Cantor

```
n=input()  
if (FIN(n,n)==0) :  
    return 1  
else:  
    return 0
```



Tõestus

- See programm ei vasta ühelegi baitkoodile
- ergo..



And it gets worse

- 1953 Rice: Ükski “huvitav” omadus pole kontrollitav
 - Mh: Programmide võrdus
 - Kas üks hangub harvem, kui teine

- Küsimusi?



Küsimused

- Programmade testimine??



Üleminek

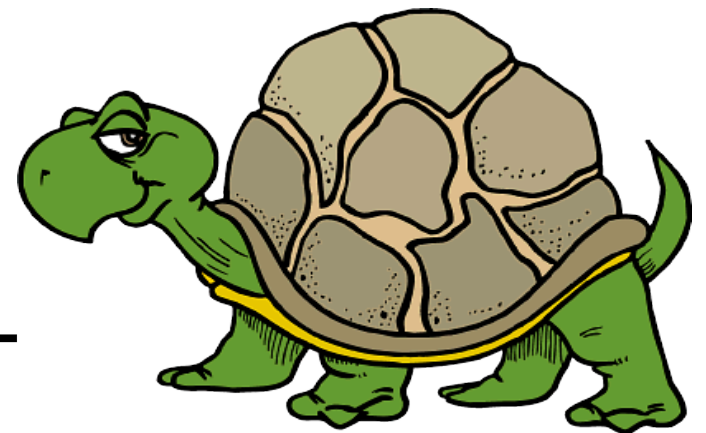
- Asjad, mida üldse ei saa
 - (Neid on veel)



Üleminek

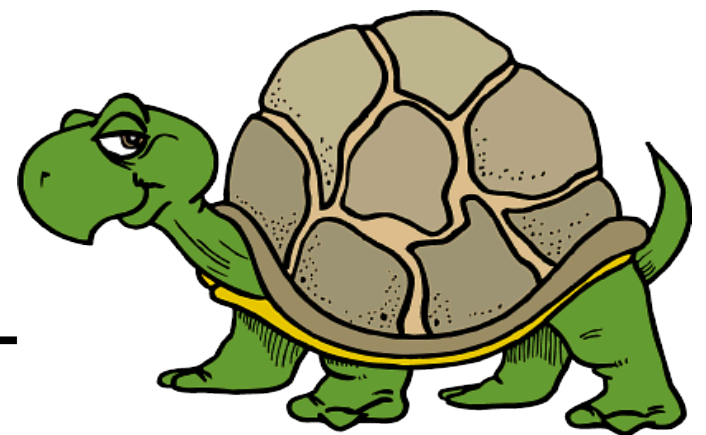
- Asjad, mida üldse ei saa
 - (Neid on veel)
- Asjad, mida nagu saaks aga...

AAEGLASELT!!!



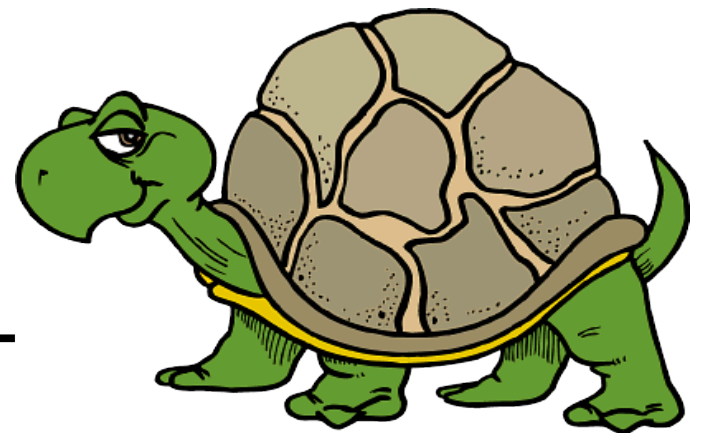
Ülesanded

- Lühim tee
- Algarvulisuse kontroll
- Ümarlaud
- Viis-tükki-ritta



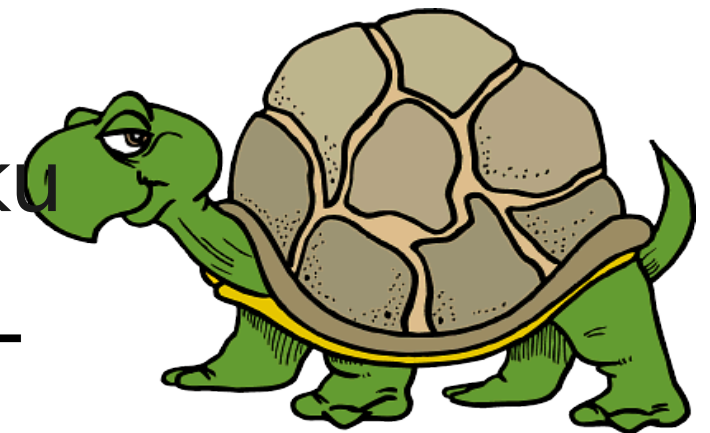
Aeglus

- Sisend eri suurusega
- Arvutamine võtab **aega**
- Aeg paraku piiratud



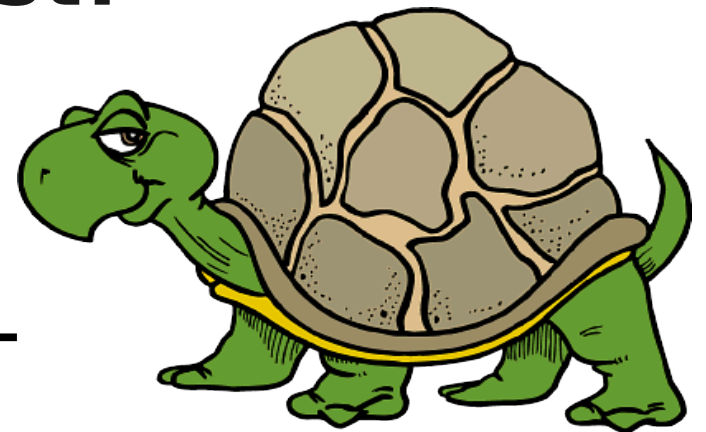
Aeglus

- Sekundis 100 000 000 = 10^8 tehet
 - Aastas $\sim 3 * 10^{15}$
 - Top 500 superarvutit sekundis $\sim 10^{16}$
 - Aastas $\sim 3 * 10^{21}$
 - Kui igaühel oleks Top 500 SA-d...
 - Aastas $\sim 2 * 10^{31}$
 - Universumi tekkest kokku $\sim 3 * 10^{40}$
-



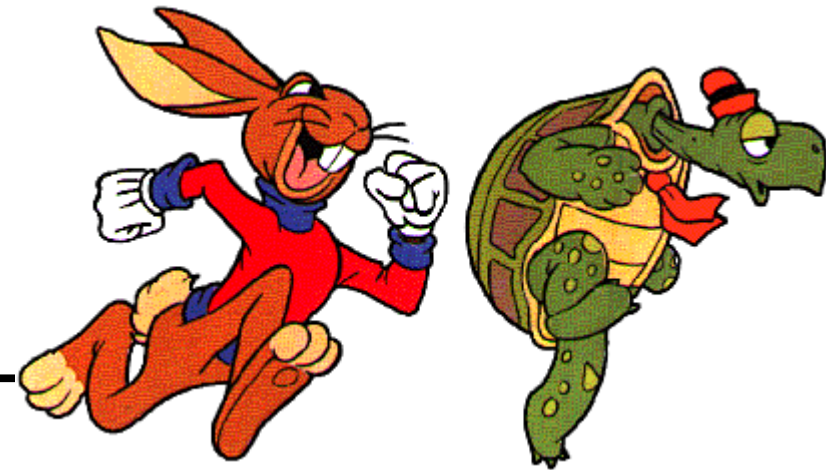
Aeglus

- Kui igaühel oleks Top 500 SA-d...
 - Aastas $\sim 2 \cdot 10^{31}$
 - Universumi tekkest kokku $\sim 3 \cdot 10^{40}$
- Võrdluseks: Rändkaupmehel 100 linna korral **$\sim 10^{160}$ võimalust!**



Seega

- Variantide läbivaatus EI TOIMI
- Teoreetiline küsimus:
 - Kas saab alati paremini?
- **P = NP ?**



Klassid

- **P** – efektiivselt lahendatavad
 - **RP** ja **BPP** – juhuslikkuse abil
- **NP** – efektiivselt kontrollitavad
- **PSPACE** – arvutis arvatavad



Tõestamisest

- **NP** – efektiivselt kontrollitavad
- Leidub 'lühike' tõestus
 - Loed läbi ja usud



Tõestamisest

- **NP** – efektiivselt kontrollitavad
- Leidub 'lühike' tõestus
 - Loed läbi ja usud
- Aga kui tervet tõestust ei viitsi?
- Tõestaja ka ei viitsi?



Tervet ei viitsi

- Vaata pool?
 - Veel parem, vaata **3 bitti**
 - Bitid vali mustri järgi juhuslikult
 - **PCP-Teoreem (1992):**
Kui leidub lühike tõestus,
leidub ka selline, kus piisab
juhuslikult 3 biti vaatamisest
-

Tõestaja ka ei viitsi

- Hää! peas:
“**Mina olen sinu JUMAL**”
 - “**Küsi ja ma vastan!**”
 - Mida paganat küsida?
 - Eriti arvestades, et ta võib valetada...
-



Vastus

- “Okei, meil on 1000 inimest, ja nad tuleb lauda paigutada...”
 - **“See pole võimalik!”**
 - Probleem
-



Vastus

- “Okei, meil on 1000 inimest, ja nad tuleb lauda paigutada...”



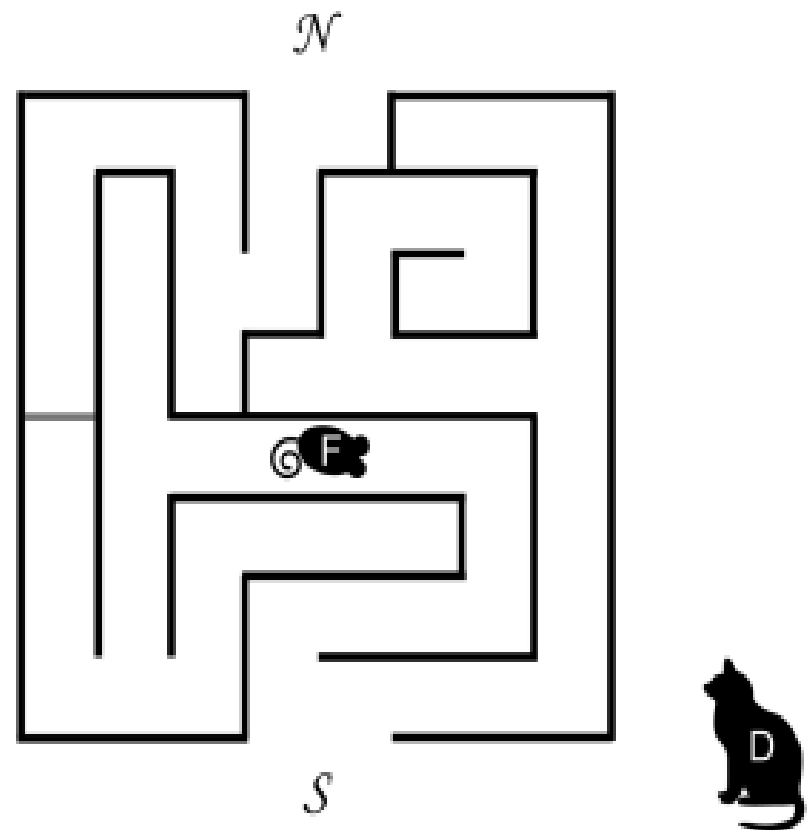
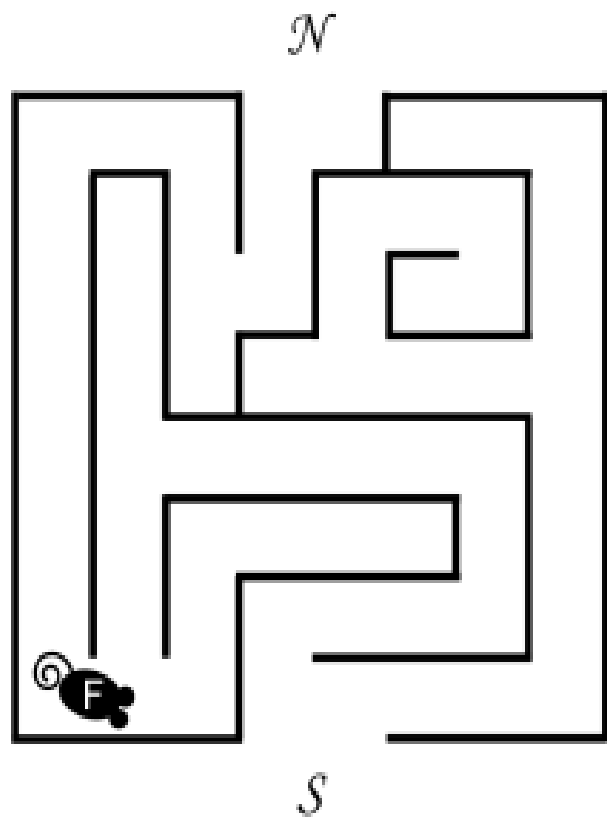
Probleemi pole

- Lühikest tõestust pole..
 - **“Ükski variant lihtsalt ei klapi”**
- Ometi on võimalik kontrollida!!
 - **PSPACE** piires



Kuidas?

- Näide: Kassi-Hiire mäng



Probleem...

**“Ei, hoopis mina olen sinu
JUMAL”**



Põhimõte

- “Kui üks on jumal ja teine pole?”
 - Mõlemad tahavad tõestada, et on jumal...
 - Mõlemal võib vabalt olla lõpmatu arvutusvõimsus...
 - Ei tee koostööd
- Informaatik vs Teoloog



Erinevus

- “Kui üks on jumal ja teine saatan siis ...”
 - Teoloog: “Kumb on kumb??”
 - Informaatik: “Saab lasta neil igasugu probleeme lahendada!!”



Mis asju?

- Kõike, mis arvutil kontrollitav on
 - Ja isegi ühtteist veel..
- Tuleb välja mõelda kuidas..
 - Aga see on mehaaniline



Kokkuvõte

- Matemaatika on kasulik
 - Kasvõi ideede mõttes
- Mõnda asja ei saa programmiga lahendada
- Häältega peas võib nalja saada



Täna tähelepanu eest!

Teil kindlasti on küsimusi!

