

Alan Turing (1912-1954)

Jaroslav Peregrin
FLÚ AV ČR & FF UHK
jarda.peregrin.cz



Matematik

1931-34: studia matematiky v Cambridge

1935-37: fellow v Cambridge

1935-37: doktorát v Princetону (pod vedením A. Churcha, autora lambda kalkulu)

1936: článek *On Computable Numbers, with an Application to the Entscheidungsproblem* (v *Proceedings of the London Mathematical Society*)

Matematik

Entscheidungsproblem (Hilbert aj.): najít
efektivní postup, kterým lze zjistit, zda je daná
formule dané teorie (například aritmetiky)
odvoditelná z axiomů této teorie

axiomatický systém je rozhodnutelný, je-li úplný

Turingovy úvahy o vyčíslitelnosti

⇒ nerozhodnutelnost aritmetiky

⇒ nerozhodnutelnost logiky 1. řádu

Matematik

Turing: abychom mohli vyřešit

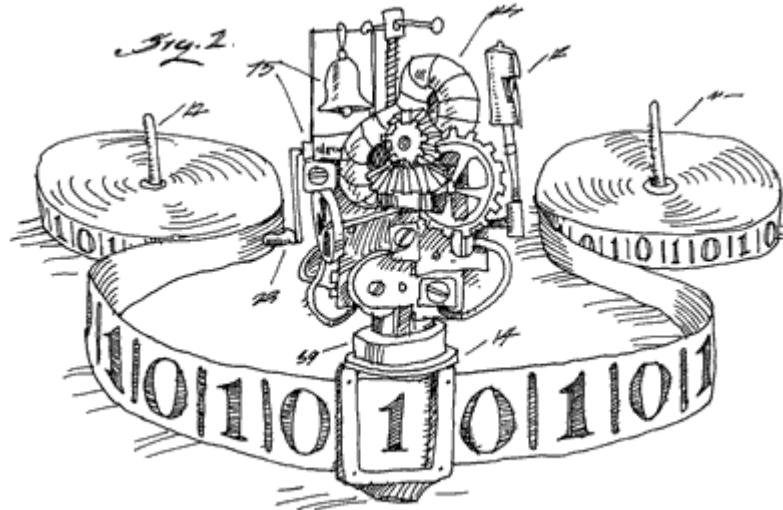
Entscheidungsproblem, musíme si udělat jasno v tom, co to je *efektivní postup*

funkce, které existují (v platónském nebi, tj. podle teorie množin)

- × funkce, jejichž hodnoty jsme fakticky schopni spočítat
- × funkce, jejichž hodnoty lze spočítat v konečném čase (= efektivní ve smyslu Turinga)

Matematik

Turingův stroj:



Matematik

Problémy neřešitelné Turingovým strojem:

- *halting problem*: zastaví se někdy daný Turingův stroj?
- *Entscheidungsproblem*

můžeme říci, že *Turingovsky* neřešitelné problémy jsou prostě neřešitelné?

Churchova teze: cokoli je vypočítatelné, je vypočítatelné Turingovým strojem

Matematik

Platí Churchova teze?

Nelze dokázat, protože tato teze propojuje
oblast formálního s oblastí neformálního

Turingovsky vypočítatelné funkce

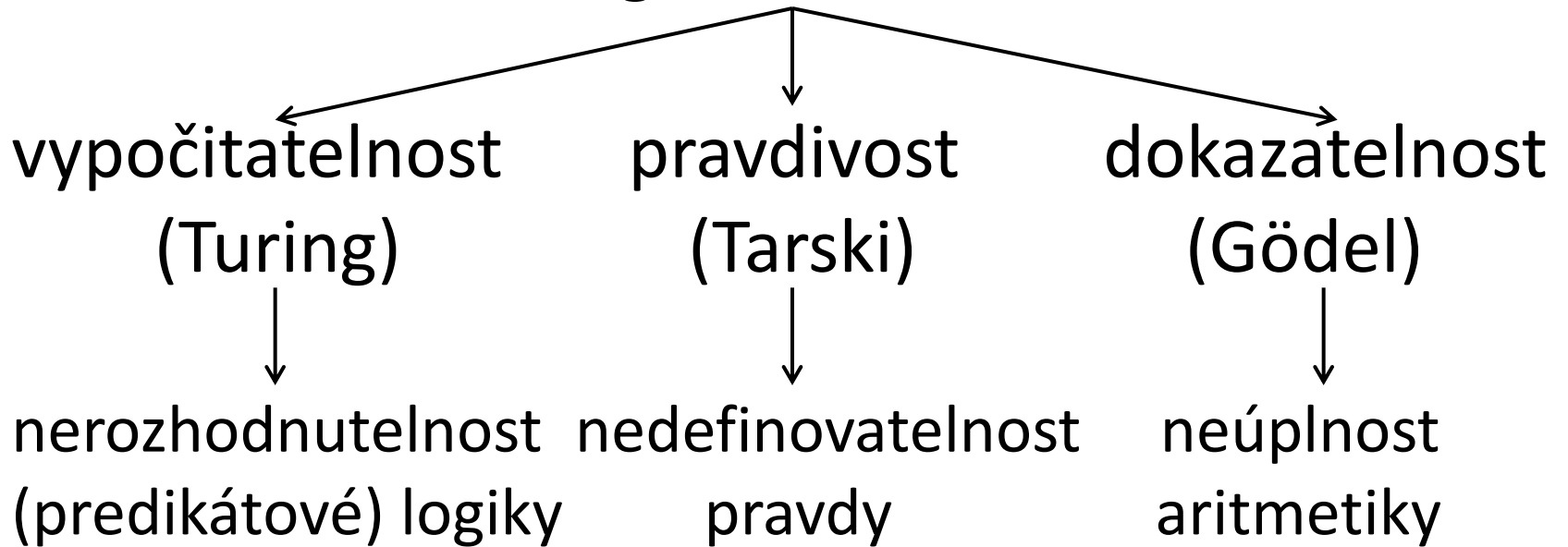
= rekurzivní funkce

= funkce reprezentovatelné v aritmetice

= funkce reprezentovatelné v lambda kalkulu

Matematik

diagonální úvaha



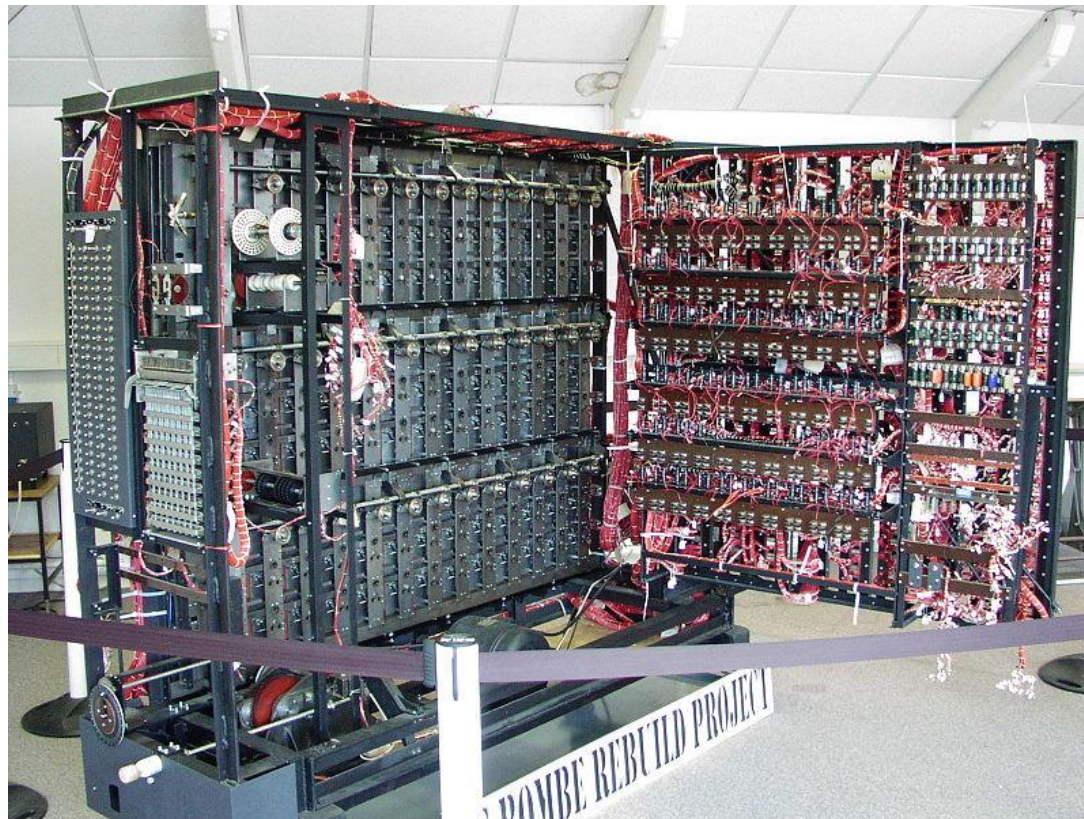
Kryptoanalytik

Od roku 1939 v Bletchley Park, centrále
"Government Code and Cypher School"
zápas s německých šifrovacím systémem Enigma



Kryptoanalytik

konstrukce "počítače"



Kryptoanalytik

prolomení německé námořní Enigmy

šéf kryptoanalytiků o Turingovi:

"Není pochyb o tom, že Turingova práce byla nejdůležitějším faktorem úspěchu našeho pracoviště. ... Na průkopnickou práci se často zapomíná, když později díky zkušenosti a rutině všechno začíná vypadat jednoduše, a mnoho z nás mělo pocit, že důležitost Turingova přínosu nebyla nikdy vnějším světem doceněna."

Počítačový vizionář

1945-47: pracuje v *National Physical Laboratory*
na "Automatic Computing Engine"

od 1948: na *University of Manchester*, práce na
počítači "Manchester Mark 1"

spolu s J. von Neumanem vyvinuli pionýrskou
koncepti *univerzálního* (programovatelného)
počítače

Počítačový vizionář

článek *Computing machinery and intelligence*,
vyšel v roce 1952 v časopise *Mind*

základní otázka: budeme moci někdy o nějakém
stroji rozumně říci, že *myslí*?

Turing: nahradíme otázku *Mohou stroje myslet?*
otázkou *mohou stroje projít určitým testem?*

⇒ "Turingův test"

Počítačový vizionář



"Úchyl"

1952: Turing byl vzat do vazby kvůli
homosexuálním stykům (kterými se příliš
netajil)

byl odsouzen a dostal na vybranou mezi vězením
a "léčbou"

podstoupil chemickou kastraci

1954: Turing spáchal sebevraždu (otráveným
jablkem)