Radek Tesař; Zbyněk Křivka; Alexander Meduna

Alan Mathison Turing – život a dílo

Pokroky matematiky, fyziky a astronomie, Vol. 59 (2014), No. 2, 89--104

Persistent URL: http://dml.cz/dmlcz/143889

Alan Mathison Turing – život a dílo

Radek Tesař, Zbyněk Křivka, Alexander Meduna, Brno

Významný britský matematik Alan Mathison Turing se dnes všeobecně považuje za jednoho ze zakladatelů informatiky, jak ji dnes se samozřejmostí přijímáme a chápeme. Proto o Vánocích (ano, přesně 24. prosince 2013) překvapila mnohé informatiky zpráva, že britská královna Alžběta II.[1] udělila tomuto géniovi milost. Čeho se vlastně Turing dopustil a proč byl odsouzen? A proč je mu milost udělena až teď – 60 let po jeho smrti? Máme-li se pokusit nalézt odpovědi na tyto otázky, musíme přehlédnout jeho život od samotného začátku...

1. Úvod

V článku vycházíme z řady pramenů, ale rádi bychom upozornili hlavně na životopis Alana M. Turinga od Andrewa Hodgese [10], jenž se věnoval životu Alana Turinga dlouhou dobu a napsal o něm několik publikací, ze kterých je nejznámější *Alan Turing: The Enigma*, která byla poprvé vydána v roce 1983, přeložena byla do mnoha jazyků a naposledy byla vydána v roce 2012. Podle této knihy napsal dramaturg Hugh Whitemore divadelní hru a později byl natočen i film *Breaking the Code*. V roce 1996 Ray Monk požádal Hodgese, aby napsal krátký text s názvem *Turing: a natural philosopher*. Ten byl vydán v roce 1997 v rámci série *The Great Philosophers*, kterou Ray Monk editoval. Práci *Turing: a natural philosopher* je možno nalézt také online na [11]. Dále se podle knihy *Alan Turing: The Enigma* točí film režírovaný Mortenem Tyldumem s Benediktem Cumberbatchem v roli Alana Turinga. Distribuce filmu *The Imitation Game* [15] je plánována na konec roku 2014. V rámci oslav 100. výročí Turingova narození vyšel také jeho medailonek od Heleny Durnové v časopise Pokroky matematiky, fyziky a astronomie [7].

Tento příspěvek jsme pojali jako popularizaci života Alana Mathisona Turinga především k jeho výročím uvedeným níže, protože většina z nás zná tohoto génia jen z učebnic informatiky jako autora Turingova stroje. Záměrně je napsán čtivou formou provokující čtenáře k dalším otázkám a diskusi o faktech zde uvedených. Pokud se nám tímto článkem podaří vzbudit ve čtenáři jiskru zájmu o Alana Turinga a problematiku jemu věnovanou, pak nebylo naše úsilí zbytečné.

Alan Mathison Turing, OBE[2], který se narodil 23. června 1912 a zemřel 7. června 1954, byl významný britský matematik, logik, kryptoanalytik a zaklada-

[1] Alžběta II. se narodila 21. dubna 1926, britskou královnou se stala po smrti svého otce Jiřího VI. 6. února 1952. Byla tedy královnou již v době zatčení a odsouzení Alana Turinga.

[2] V roce 1945 byl udělen Turingovi řád britského impéria (angl. zkratka OBE).

Ing. Radek Tesař, Ing. Zbyněk Křivka, Ph.D., prof. RNDr. Alexander Meduna, CSc., Fakulta informačních technologií, Vysoké učení technické v Brně, Božetěchova 1/2, 612 66 Brno, e-mail: {itesar, krivka, meduna}@fit.vutbr.cz

Obr. 1. Alan M. Turing

tel moderní informatiky. V roce 2012 by byl oslavil 100. narozeniny a v letošním roce si pak připomeneme 60. výročí jeho úmrtí.

Alan Turing (obrázek 1) se narodil v Paddingtonu (Londýn) v době dovolené jeho otce, který pracoval pro indickou veřejnou správu (ICS) v Chhatapuru, Biharu a provincii Orissa v Britské Indii. Alan měl také o tři roky staršího bratra Johna. Rodiče Julius Mathison a Ethel Sara Turingovi žili téměř do synova narození, a pak i později v indickém Madrásu[3], kde se seznámili a kde byl Alan i počat. Julius a Ethel však chtěli, aby jejich děti byly vychovány v Anglii. Julius Mathison Turing (1873–1947), jenž měl titul baroneta, byl syn kněze ze skotské rodiny obchodníků, která pocházela z Holandska. Jeho dědeček byl generál v bengálské armádě. Ethel Sara Turingová (rozená Stoneyová, 1881–1976) byla dcera Edwarda Waller Stoneye, hlavního inženýra Madráských železnic. Rodina Stoneyů byla protestantská anglo-irská šlechtická rodina pocházející z obou hrabství Tipperary a hrabství Longford, zatímco Ethel sama strávila většinu svého dětství v hrabství Clare. Z této rodiny pocházelo v 19. století hned několik významných fyziků a inženýrů.

Poté, co se Alan Turing narodil, se jeho otec vrátil z Anglie zpět do Indie a matka jej následovala o rok a půl později, ale malého Alana s sebou nevzali. Ani on, ani jeho bratr Indii nikdy nenavštívili. Alana i jeho bratra Johna vychovávali chůvy a příbuzní. Když Alanův otec předčasně odešel do výslužby, oba rodiče opustili Indii a z daňových důvodů se usadili na francouzské straně kanálu La Manche, kde je oba jejich synové navštěvovali pouze o Velikonocích, o letních prázdninách a o Vánocích. Alan měl i přesto k matce velmi blízký vztah.

Alan ve svém dětství nevykazoval výjimečnou inteligenci, byl průměrným žákem. Bavily ho šachy, ale nebyl zvlášť dobrým hráčem. Ve věku 14 let se dostal na střední školu v Sherborne, ale v den, kdy měl nastoupit, se konala generální stávka dopravců.

[3]Madrás je od roku 1996 nazýván Čennaj.

Rozhodl se tedy, že do školy pojede ze Southamptonu na kole. Na tom by nebylo nic zvláštního, kdyby vzdálenost nečinila přibližně 100 km. O jeho výkonu se pak psalo i v místních novinách. Škola v Sherborne mladého Turinga zklamala. Byl neohrabaný ve vztazích se spolužáky a učiteli, proto se často stával terčem posměchu. Jediné, co ho zajímalo, byly přírodní vědy. Nadchla ho také chemie, ale hlavně matematika, o které dokonce později prohlásil, že mu poskytuje sexuální potěšení.

I přes kritiku učitelů Turing často vytvářel vlastní postupy řešení problémů. Pro své nekonvenční myšlení Turing vyhrával téměř všechny matematické soutěže v Sherborne. V chemii, která ho zaujala od velmi útlého věku, prováděl své vlastní pokusy. Těm se pak věnoval v průběhu celého svého života a ve své chemické laboratoři trávil hodně času. Během své školní docházky se také věnoval pokročilé matematice, ale jeho učitelé o jeho zájmech neměli zřejmě ani nejmenší tušení. Alan Turing v té době četl práce Alberta Einsteina o speciální a obecné teorii relativity a práci *The nature of the physical world* (Podstata fyzikálního světa) Arthura Stanleyho Eddingtona o kvantové mechanice.

Na škole se seznámil s Christopherem Morcomem, který studoval ve vyšším ročníku a s nímž ho pojilo hluboké přátelství. Toto přátelství z Alanovy strany později přecházelo v mnohem hlubší city. Zde si pravděpodobně poprvé uvědomil své homosexuální zaměření. Společně diskutovali o vědeckých novinkách a prováděli vlastní pokusy. Když v roce 1930 Morcom zemřel na tuberkulózu, byla to pro Turinga rána, z níž se těžko vzpamatovával. Po ztrátě přítele se rozhodl plně věnovat vědě. Požádal Christopherovu matku o fotografii přítele a poté, co ji obdržel, napsal v dopise matce: „Dívá se na mne z mého stolu a povzbuzuje mě k tvrdé práci.“ Protože Morcom byl před svou smrtí přijat na Cambridge, rozhodl se Alan naplnit jeho odkaz. Podle svých slov chtěl učinit objevy, které by jinak jistě učinil Morcom. Prožitek z přítelovy smrti byl pro něj také impulsem k zamyšlení, co přežije člověka po jeho smrti a zda by nebylo možné nějak zachovat alespoň lidského „ducha“. To později vedlo k jeho zájmu o umělou inteligenci. Není bez zajímavosti, že v tomto kontextu je Turingův odkaz i přes relativně nízký dožitý věk velmi významný nejen pro informatiku a matematiku, ale také pro další obory. I když zemřel již ve 42 letech, zanechal po sobě velké myšlenky i důležité výsledky, což mu bezpochyby zaručuje nesmrtelnost.

V armádní škole pro důstojníky získal Alan hodnost seržanta. Po celý život byl nadšeným sportovcem, obzvlášť vynikal v běžích na dlouhé trati a při maratonu. Přestože byl vynikajícím sportovcem, nikdy nebyl přijat do reprezentace.

Rok po Morcomově smrti byl přijat na proslulou King's College v Cambridgi. Byla to zlatá léta, kdy zde působili Bernard Russell, Alfred North Whitehead a Ludwig Wittgenstein. Den co den se zde odehrávaly debaty o zásadních otázkách matematiky a logiky. Turing byl sice nenápadným, ale velice pilným studentem, jemuž nechyběl vhled do podstaty řady problémů. V Cambridgi jej od roku 1933 začala zajímat matematická logika, a proto zde v Morálním vědeckém klubu v prosinci téhož roku přečetl svoji práci *Matematika a logika*, v níž tvrdil, že na matematiku se nelze dívat jen čistě logicky, ale že matematika vyžaduje různé interpretace, jichž nelze logikou dosáhnout.

V letech 1931 až 1934 studoval hlavně matematiku a v roce 1935 byl zvolen členem univerzitní koleje (fellow) na základě své disertace *On the Gaussian error function* (O Gaussově chybové funkci), v níž dokázal některé zásadní věty teorie pravděpodobnosti jako je centrální limitní věta. Přestože centrální limitní věta byla

objevena krátce před Turingovou prací, Turing tuto větu objevil a dokázal nezávisle. V roce 1936 obdržel Smithovu cenu[4]. Turingovo zaměření a vědecký přínos se tak netýká pouze informatiky [3], i když je v této oblasti nejvýznamnější.

Na jaře roku 1935 začal navštěvovat přednášky Maxe Newmana o základech matematiky, kde se seznámil s prací Kurta Gödela o neúplnosti a s Hilbertovým problémem rozhodnutelnosti. V určitém smyslu je „rozhodnutelnost" jednoduchým problémem, protože jejím úkolem je rozhodnout, zda určité tvrzení je pravdivé nebo nepravdivé. Pro řadu tvrzení lze snadno nalézt potřebný algoritmus, problém však nastává v okamžiku, kdy potřebný algoritmus nelze nalézt. Pokud nějaký postup problém řešil, pak skutečně šlo o algoritmus, přestože přesná definice ještě neexistovala. Turing se začal těmito myšlenkami zabývat.

V té době byl Turing oceněn především za svoji práci v teorii pravděpodobnosti, ačkoliv intenzivně pracoval na problémech rozhodnutelnosti a navštěvoval Newmanovy přednášky. Jeho největší vědecké zásluhy však tkví v jeho článku *On Computable Numbers, with an Application to the Entscheidungsproblem* z roku 1936 [17]. Zavedl v něm pojem Turingova stroje, teoretického modelu obecného výpočetního stroje, který se stal jedním ze základů informatiky, a dokázal, že problém zastavení Turingova stroje není rozhodnutelný. Na základě Churchovy–Turingovy teze pak lze toto zjištění aplikovat na Hilbertem formulovaný tzv. Entscheidungsproblem neboli problém rozhodnutelnosti. Gödel zveřejnil v roce 1931 věty o neúplnosti, které matematiky tehdejší doby doslova šokovaly. První Gödelova věta říká, že v žádné rozumné teorii hovořící o přirozených číslech není dokazatelné vše. Druhá Gödelova věta dává konkrétní příklad takového nedokazatelného tvrzení pro Peanovu aritmetiku – je jím věta „Peanova aritmetika je bezesporná". Turing však svým strojem dokázal, že Gödelova tvrzení jsou pravdivá.

Není bez zajímavosti, že Turing vycházel z prací svého krajana Charlese Babbage, jenž se již v 19. století pokoušel zkonstruovat počítač. Byl to „Difference Engine" a později „Analytical Engine", který se stal prvním univerzálním turingovsky úplným počítačem. Turingův článek *On Computable Numbers, with an Application to the Entscheidungsproblem* rovněž obsahuje teoretický základ ke konstrukci počítače a k programování.

Přestože Turingova práce [17] je revoluční pro informatiku, její publikování v časopise *Proceedings Londýnské matematické společnosti* nebylo bez komplikací. Ve stejném roce jen o několik měsíců dříve totiž publikoval Alonzo Church v odborném časopise the *American Journal of Mathematics* článek, ve kterém dokázal, že v aritmetice neexistuje žádná rozhodovací procedura. Turingův příspěvek se od této práce sice výrazně lišil, Newman však přesto v matematické společnosti argumentoval proti jeho uveřejnění. Turing pak svůj článek doplnil o odkazy na Churchovy výsledky a poprvé jej zveřejnil v dubnu 1936, a pak následně ještě jednou upravený v srpnu 1936.

V roce 1936 se Turing stal postgraduálním studentem na Princetonské univerzitě a v letech 1937–1938 zde trávil většinu času. Byl členem výzkumného týmu matematických logiků vedených Alonzem Churchem. Pracoval mimo jiné na komplexní analýze a Riemannově funkci zeta. V roce 1938 dokončil svoji práci o logice a obhájil doktorát.

[4]Cena udílená na univerzitě v Cambridgi, kterou obdrží každý rok dva nebo více studentů bakalářského studia za nejpřínosnější práci v matematice a přírodních vědách. Cena byla každoročně udílena v letech 1769–1998, mimo 1917. V roce 1998 byla nahrazena cenou Smitha-Knighta a Rayleigha-Knighta

V Princetonu také v roce 1939 publikoval svoji významnou práci *Systems of Logic Based on Ordinals* (Logické systémy založené na ordinálech). V Princetonu se setkal s Johnem von Neumannem a G. H. Hardym, o kterém se vědělo, že je také gay, o letních prázdninách v roce 1937 se zde poprvé setkal s L. Wittgensteinem. V Princetonu napsal dva články týkající se matematiky. První se zabýval metodami aproximace Lieových grup konečnými grupami a druhý rozšířením těchto grup. Po obhájení doktorátu mu von Neumann na základě výsledků jeho výzkumu publikovaného v uvedených článcích nabídl místo. Turing však odmítl a raději se vrátil do Británie a zapojil se do války.

V letech 1938–1939 však stihl ještě rozpracovat svůj stroj na počítání netriviálních nulových bodů funkce zeta, hádat se s Ludwigem Wittgensteinem o filozofii matematiky a také v době mnichovské dohody začít pracovat pro vládu na problému dešifrování německé komunikace. Po začátku války Turing nastoupil do Bletchley Parku, kde v práci na dešifrování nepřátelské korespondence pokračoval.

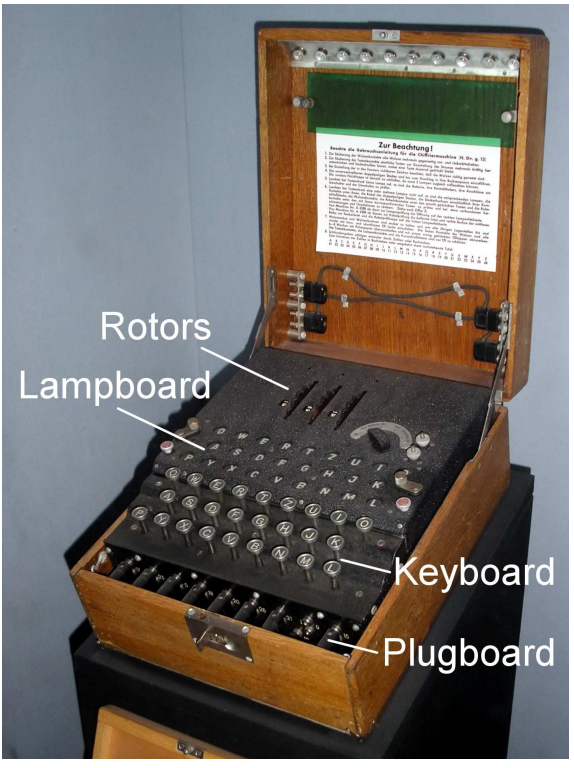
V Cambridge, kde bylo relativně liberální prostředí v kontrastu s ostatní britskou společností, prožil Turing zřejmě nejkrásnější léta svého života. Po vypuknutí druhé světové války se všechno změnilo. Protože byl schopným matematikem (byl již členem King's College), o němž se hovořilo v intelektuálních kruzích, byl mu svěřen velmi náročný úkol podílet se na luštění tajných německých šifer. Za druhé světové války byl Turing jedním z nejdůležitějších vědců, kteří v Bletchley Parku luštili německé tajné kódy šifrované stroji Enigma a Tunny. Toto snažení bylo velice úspěšné a Angličané měli po větší část války k dispozici většinu z tajné nepřátelské komunikace. Tak jako jiní pracovníci v Bletchley Parku Turing nebyl nijak veřejně oceněn, a dokonce o své práci nemohl ani mluvit, jelikož by tím porušil státní tajemství. Počítač Colossus, na kterém pracoval a který sloužil k luštění šifry Lorenz kódované stroji Tunny, byl po válce na povel Winstona Churchilla zničen. Později, již po Turingově smrti, bylo napsáno, že Turingova práce na analýze tajných kódů během druhé světové války byla nejdůležitějším příspěvkem jednotlivce k vítězství Spojenců.

2. Enigma

Nejdůležitější část Turingova života se odehrávala za války, kdy v Bletchley Parku prováděl kryptoanalýzu. Zde se také dočkal největšího uznání kolegů a byla to práce, která jej zcela pohltila. Pro její pochopení však musíme trošku odbočit a začít ještě před válkou.

Německý vynálezce Arthur Scherbius získal roku 1918 patent na šifrovací přístroj Enigma (obrázek 2). V letech 1925–1945 se těchto přístrojů prodalo německé armádě přes 30 000 kusů.

Ve svém principu se jedná o poměrně důmyslný přístroj, jehož základem je 26tlačítková klávesnice jako na psacím stroji, sada 26 žárovek prosvětlující písmena rozmístěná stejně jako zmíněná klávesnice, propojovací deska, tři rotory a reflektor. Stisknutím klávesy na klávesnici dojde k sepnutí spínače a proud projde z baterie do prvního rotoru, kde se toto odpovídající písmeno nahradí (substituuje) jiným, v dalším rotoru zase jiným, stejně jako ve třetím. Reflektor pak funguje jako statický rotor, kde se opět písmeno nahradí a vrací se zpět do rotorů. Kontakty prvního rotoru jsou pak propojeny s jednotlivými žárovkami odpovídající danému písmenu. Díky tomu proud po průchodu Enigmou rozsvítí žárovku, která odpovídá zašifrovanému písmenu.

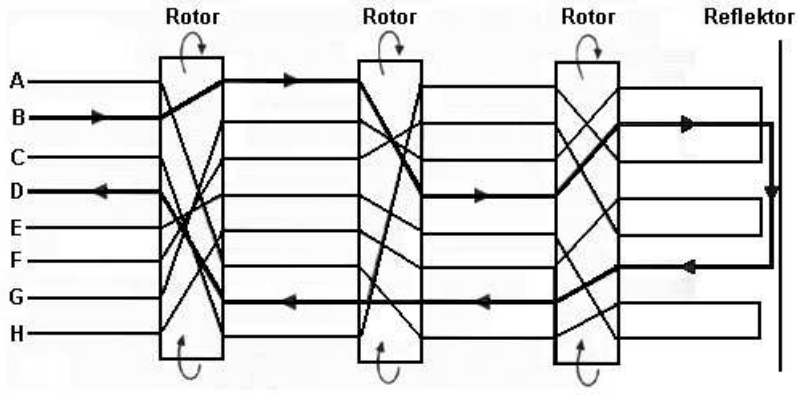


Obr. 2. Enigma

Obrázek 3 znázorňuje průběh šifrování, kdy je písmeno B substituováno na D. Nejzajímavější na celé věci ale je, že první rotor se po každém stisku klávesy pootočí o jednu pozici, takže následujícím stiskem stejné klávesy dostaneme jiné zašifrované písmeno. Pokud se první rotor otočí o jednu otáčku (po 26 stiscích kláves), druhý se pootočí o jednu pozici. Pokud se otočí druhý rotor o jednu otáčku, třetí se pak posune také o jednu pozici. Díky tomu získáme $26^3 = 17\,576$ odlišných nastavení.

Pro šifrování je tedy nutno nastavit rotory do výchozí pozice, kterých je celkem 17 576, čímž se určí, jak bude Enigma zprávu šifrovat. Toto nastavení odpovídá šifrovacímu klíči a bylo určeno kódovou knihou, kde pro každý den bylo určeno jiné nastavení rotorů. Pro čtyři týdny tedy potřebujeme kódovou knihu s 28 nastaveními. Operátor podle této knihy nastaví Enigmu, na klávesnici napíše první písmeno zprávy, podívá se, které písmeno se rozsvítilo, a zapíše první znak zašifrovaného textu. Takto napíše celou zprávu a následně ji odvysílá. Příjemce nastaví svoji Enigmu podle stejné kódové knihy, zadá první písmeno zašifrovaného textu a zapíše si, které písmeno se mu rozsvítilo. Právě díky reflektoru je celá operace inverzní, tzn., že na obrázku 3 se písmeno D nahradí písmenem B. To má však ještě jednu vlastnost, které pak bylo využito při kryptoanalýze: nikdy se nemůže nějaké písmeno substituovat sebou samým.

Pokud neznáme kódovou knihu, musíme při kryptoanalýze postupovat následovně: náhodně nastavíme rotory, zapíšeme část rozšifrovávaného textu a zkontrolujeme, zda-li je rozšifrovaný text smysluplný. Pokud ne, nastavíme další kombinaci rotorů



Obr. 3. Schéma zapojení rotorů

a celý proces opakujeme. Takto bychom v nejhorším případě museli vyzkoušet všech 17 576 kombinací, což při zapojení více kryptoanalytiků není nereálné. Proto Scherbius udělal rotory výměnné, díky čemuž je možno pozici rotorů měnit (první rotor místo třetího atd.). To nám dává celkem $6 \times 17\,576$ kombinací. Později pak měli vojáci k dispozici sadu celkem 5 rotorů, takže mohli použít libovolné 3 z pěti rotorů.

Další novinkou bylo použití propojovací desky. Ta byla zapojena mezi klávesnici a první rotor. Zde bylo možno prohodit vždy dvě písmena mezi sebou (např. A a B). Takto se prohazovalo šest libovolných dvojic písmen, ostatních 14 písmen zůstalo neprohozených. Tím bylo získáno dalších 100 391 791 500 kombinací. Celkově se tím zvýšil počet možností na více než 10^{16} (při použití pouze tří rotorů!) a Scherbius nabyl přesvědčení, že je Enigma nezdolatelná.

2.1. Luštění Enigmy

Luštění Enigmy začalo v Polsku ještě před druhou světovou válkou. Polské Biuro Szyfrów mělo sice k dispozici komerční verzi Enigmy, ta se ale lišila od vojenské hlavně v zapojení rotorů, a proto nebyla použitelná pro luštění vojenských kódů. Zde však pomohla náhoda v podobě Hanse-Thila Schmidta. Jeho bratr byl náčelníkem štábu spojovacích jednotek a byl to on, kdo schválil nasazení Enigmy v německé armádě. Hans-Thilo byl bez prostředků a proto musel požádat bratra o pomoc. Ten mu zajistil místo v berlínském Chiffrierstelle – velitelském centru sítě přístrojů Enigma.

Hans-Thilo záviděl bratrovi jeho úspěšnou kariéru, a proto se mu rozhodl pomstít a zároveň si tím i přivydělat. Dne 8. listopadu 1931 si dal v hotelu Grand v belgickém Verviers schůzku s francouzským tajným agentem s krycím jménem Rex. Tomu nechal za 10 000 marek ofotit návody k použití Enigmy, ze kterých se dalo odvodit zapojení rotorů. To však ke kryptoanalýze nestačí, je totiž nutno vědět, kterou z více než 10^{16} kombinací nastavení přístroje použít. Německé memorandum to shrnulo slovy: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici.“

Na základě deset let staré smlouvy mezi Poláky a Francouzi o vojenské spolupráci jim Francouzi předali všechny informace o Enigmě. Součástí informací byl i popis, jak vypadají kódové knihy. Němci totiž zavedli opatření pro ztížení možné kryptoanalýzy, kdy se pomocí denního klíče kódoval pouze klíč zprávy. Ten měl stejné nastavení pro-

pojovací desky i pozici rotorů, ale lišil se v nastavení rotorů. Nejprve odesílatel nastavil Enigmu na denní klíč (např. QCW), zakódoval jím nový klíč zprávy (např. PGH), který zakódoval 2× po sobě, aby se vyloučila možnost chyby. Takže prvních šest znaků zprávy bylo PGHPGH, což se zakódovalo jako KIVBJE. Zbytek zprávy pak kódoval s nastavením rotorů na PGH. Příjemce tedy prvních šest znaků KIVBJE dešifroval pomocí denního klíče (QCW), tím získal otevřený text PGHPGH, nastavil rotory na PGH a teprve pak dešifroval zbytek zprávy.

V této době pracoval v Biuru Szyfrów třiadvacetiletý matematik Marian Rejewski, který začal analyzovat Enigmu. Nejprve sestrojil repliku vojenské verze. Dále věděl, že prvních šest písmen jsou dvakrát opakovaná tři písmena klíče zprávy, proto se na ně zaměřil. V předchozím případě se PGH zobrazilo na KIV a druhé PGH na BJE. V prvním případě se P zobrazilo na K, v druhém na B. Rejewski zjistil, že pokud má dost zpráv, je schopen vytvořit celou abecedu vztahů, kde na prvním řádku bylo K, v druhém řádku pod ním B atd. Z toho pak vytvořil řetězce tak, že např. K se zobrazí na B, B se zobrazí na jiné písmeno a to se zobrazí opět na K. Tím získal řetězec délky tři. Pokud to provedl se všemi znaky abecedy, dostal několik řetězců různé délky. Dále pak rozdělil problém analýzy na nastavení rotorů a nastavení propojovací desky. Propojovací deska neměla na délku řetězce žádný vliv, znamenala jen záměnu některých písmen. Zaměřil se tedy na délku a počet řetězců, které ovlivňovaly pouze rotory. Tím snížil náročnost analýzy na $6 \times 17\,576$, což je 105 456 možností. Poté se svým týmem sestavil katalog délek a počtu řetězců, což znamenalo vyzkoušet všech 105 tisíc kombinací. To mu zabralo celý rok, ale pak byl schopen pomocí katalogu najít správné nastavení Enigmy ihned po té, co vytvořil abecedu vztahů toho dne a z ní dostal počet a délku řetězců.

Nakonec zbývalo dešifrovat zapojení propojovací desky. Pokud dešifroval text zprávy, dostal částečně čitelný text, například „plijedtedobelrina“. To pravděpodobně znamená „prijedte do berlina“. To tedy znamená, že R a L jsou propojena, ale A, I, E, B a N nejsou. Analýzou dalších vět pak mohl určit další písmena, která bylo nutno prohodit. Tímto postupem mohl dešifrovat německou korespondenci ve stejný den, kdy byla odvysílána. Později pak sestavil mechanickou verzi svého katalogu délek řetězců, takzvanou bombu (tento mechanický stroj vydával při své činnosti hlasitý tikot). Potřeboval šest jednotek, každou pro jedno z možných uspořádání rotorů, které pracovaly paralelně. Každá jednotka tedy prošla během dvou hodin všech 17 576 kombinací a našla tu správnou.

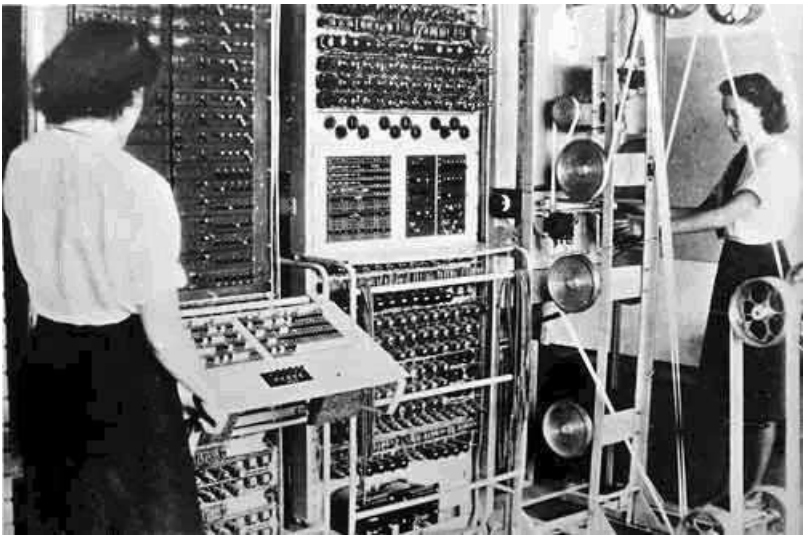
V roce 1938 Němci zvýšili bezpečnost Enigmy tím, že všem operátorům dodali dva nové rotory. Do Enigmy bylo možno umístit kterékoliv tři z pěti rotorů v libovolné kombinaci. Tím se zvýšil počet uspořádání na 60. Rejewski by tedy musel postavit 10× více bomb, aby je byl schopen dešifrovat, což bylo pro Poláky příliš drahé. Navíc Němci přidali další čtyři propojovací kabely, a tím měnili celkem dvacet písmen. Šéf Biura Szyfrów usoudil, že spojenci by si mohli dovolit postavit více bomb, proto pozval šéfy francouzské a britské kryptoanalýzy a předvedl jim funkční bombu. S tím jim také nabídl detailní plány na výrobu bomb a dvě funkční repliky Enigmy. Ty pak skončily v Anglii v Bletchley Parku, v sídle Government Code and Cypher School (GC&CS). Není bez zajímavosti, že Marian Rejewski po německé invazi do Polska uprchl přes Francii do Británie, kde se zapojil do kryptoanalýzy nepřátelské komunikace. Protože byl původním autorem dešifrování Enigmy, zdálo se přirozené, že by

se měl stát součástí týmu luštitelů v Bletchley Parku. Místo toho však byl poslán luštit méně důležité šifry do malé zpravodajské jednotky v Boxmooru u Hemel Hempsteadu. O významu a vlivu své práce nevěděl až do léta 1974, kdy kapitán F. W. Winterbotham dostal povolení napsat knihu *The Ultra Secret* o Bletchley Parku. F. W. Winterbotham byl za války v Bletchley zodpovědný za distribuci informací Ultra.

Dne 4. září 1939 nastoupil do Bletchley Parku Alan Turing a hned se vrhl na rozvíjení práce Rejewského. Ta vycházela z faktu, že operátoři vysílali klíč zprávy dvakrát po sobě, což snižovalo bezpečnost Enigmy. Dalo se očekávat, že si toho Němci časem všimnou a přestanou klíč zprávy opakovat. Turing si všiml, že za dobu dešifrování Enigmy nashromáždili rozsáhlou knihovnu dešifrovaných textů, které měly často pevný protokol. Např. každé ráno v 6 hodin posílali Němci zprávy o počasí, takže o zprávě po šesté ráno mohl s určitostí říct, že na konkrétním místě bude mít slovo Wetter (počasí). Takové vazbě se říká tahák (crib). Turing byl přesvědčen, že tyto taháky mu umožní rozluštit Enigmu. Napodobil tedy Rejewského a rozhodl se pro podobné smyčky, které ale neměly nic společného s klíčem zprávy. Navíc musel eliminovat vliv propojovací desky. Vytvořil tak zařízení vzdáleně připomínající Rejewského bombu. Zvěst o jeho průlomu znamenala, že vedoucí kryptoanalytici GC&CS začali považovat Turinga za prvotřídního odborníka a génia, ale nikdo mimo GC&CS neměl ani ponětí o Turingově pozoruhodném výkonu, protože vše, co souviselo s Bletchley Parkem, bylo přísně tajné. Ani Turingovi rodiče neměli ponětí, co Alan vlastně dělá. Byl nadšen kryptoanalýzou a jmenován hlavním kryptoanalytikem. 14. března 1940 dorazil první prototyp bomby nazvaný Victory, který však nesplnil očekávání, takže jej Turing přepracoval. Dne 1. května 1940 se stalo to, co Turing očekával – Němci přestali opakovat klíč zprávy, a tím rapidně poklesla úspěšnost dešifrování zpráv až do 8. srpna téhož roku, kdy dorazila nová bomba pojmenovaná Agnus Dei. Podle sira Harryho Hinsleye zkrátila Turingova práce válku nejméně o tři roky a byly díky ní zachráněny tisíce životů. Nebýt jeho, muselo by se vylodění v Normandii odložit nejméně o rok [14].

Němci však nespoléhali jen na Enigmu. Měli také mnohem sofistikovanější šifru Lorenz, kterou šifrovali pomocí stroje jménem Tunny. První zprávy šifrované Tunny byly zachyceny v červnu 1941. Jednalo se o tzv. Teleprinter, kde operátor zadával na klávesnici otevřený text, zařízení jej automaticky šifrovalo a na druhé straně pak vystupoval opět otevřený text. Souhrnně nazývali v Bletchley takové šifrovací stroje jménem Fish. Kryptoanalýza této šifry byla velmi náročná, proto Turing sestrojil první elektronický počítač na světě, který dostal název Colossus (obrázek 4).

Konstrukci tohoto počítače zahájil A. Turing s Thomasem H. Flowersem, který byl nejprve jeho asistent, v lednu roku 1943 a již v prosinci téhož roku jej uvedli do provozu. Byl sestaven z 1 800 elektronek a jednalo se o první programovatelný počítač na světě, i když byl v určitém ohledu limitován (neuměl například desítkové násobení). Protože vše, co se týkalo GC&CS bylo přísně tajné, byl Colossus po válce zničen a nesmělo se o něm mluvit ani psát [10]. Proto bylo prvenství elektronického počítače přiřknuto univerzitě v Pensylvánii, kde v letech 1943 až 1946 vytvořili Electronic Numerical Integrator and Computer (ENIAC). Zkonstruovali jej John William Mauchly a J. Presper Eckert Jr. Pro porovnání – byl složen z 18 000 elektronek a potřeboval 150 kW příkonu! Také údržba byla velmi náročná, protože každý den bylo nutno najít a vyměnit asi 50 vadných elektronek.



Obr. 4. Colossus

Od listopadu 1941 do března 1942 byl Turing vyslán britskou vládou do Spojených států amerických, aby se zde podílel na dekódování německých zpráv a na systému utajování hovorů. Německé námořnictvo později změnilo své kódy a kryptoanalytici v Bletchley Parku ztratili možnost německé zprávy dekódovat. Turing se již přímo nepodílel na rozluštění těchto složitějších kódů, ale jeho myšlenky byly pro tuto práci významným přínosem. V roce 1945 byl Alan Turing za tento svůj přínos vyznamenán.

Po válce bylo GC&CS rozpuštěno a britské dešifrovací aktivity převzalo Government Communication Headquaters (GCHQ) v Londýně, které dále zaměstnávalo Turinga až do roku 1952, kdy mu byl v důsledku obvinění z homosexuality odepřen přístup k tajným informacím a již pro vládu nesměl pracovat.

3. Funkce zeta

Turing se zabýval Riemannovou funkcí zeta a hledáním netriviálních nulových bodů již jako student, ale kvůli válce musel výzkumu zanechat, proto se první tištěné zmínky o jeho práci na toto téma objevily až po válce [18]. Nejvíce ho zajímalo rozmístění prvočísel v číselné řadě, což souviselo s jeho zájmem o kryptografii. Již od počátku měl pochybnosti o platnosti Riemannovy hypotézy a v průběhu času byl vůči její platnosti stále skeptičtější. Dlužno podotknout, že v době před druhou světovou válkou byla nedůvěra v platnost Riemannovy hypotézy celkem běžná.

Riemannova hypotéza se týká netriviálních nulových bodů funkce zeta $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ a tvrdí, že všechny tyto body (kterých je nekonečně mnoho) leží ve středu kritického pásu $0 < \operatorname{Re} s < 1$, tedy že $\operatorname{Re} s = \frac{1}{2}$. Mimo netriviální nulové body existují ještě triviální nulové body, které jsou $s = -2, -4, -6, \ldots$ [9].

Ve třicátých letech obdržel E. C. Titchmarsh grant na výpočet nulových bodů funkce zeta. Ve spolupráci s L. J. Comriem sehnal několik mechanických kalkulaček

(tabulating machines) a několik „computers“ (tak v té době nazývali operátory mechanických kalkulaček, většinou to byly ženy). S jejich pomocí pak spočítal, že ze 1 041 nulových bodů v rozsahu $0 < \operatorname{Im} s < 1\,468$ všechny vyhovují Riemannově hypotéze.

Ještě před válkou chtěl Turing rozšířit Titchmarshův výsledek, a proto začal pracovat na stroji, který měl počítat netriviální nulové body funkce zeta v rozsahu $0 < \operatorname{Im} s < 6\,000$, kterých je 5 598. Částečně ho inspiroval stroj na předpovídání přílivu v Liverpoolu. Na tento stroj obdržel grant 40 liber od Královské společnosti. Práce na tomto stroji byla přerušena druhou světovou válkou a později nebyl nikdy dokončen.

Po válce pak začaly být dostupné elektronické počítače a Turing byl první, kdo je využil k výpočtu funkce zeta. V roce 1950 k tomu použil počítač Manchester Mark I a rozšířil Titchmarshův výsledek na prvních 1 104 netriviálních nulových bodů v rozsahu $0 < \operatorname{Im} s < 1\,540$. Toto rozšíření bylo tak malé proto, že nebylo možné udržet počítač v provozuschopném stavu delší dobu. Tyto netriviální nulové body počítal Manchester Mark I od tří hodin odpoledne do osmi hodin ráno.

Důležitější než tento výpočet netriviálních nulových bodů je však Turingův předválečný výpočet 1 054 nulových bodů v rozsahu $2\pi \times 63^2 \geq \operatorname{Im} s \geq 2\pi \times 64^2$, které všechny leží na kritické přímce. Dlužno podotknout, že $2\pi \times 63^2$ je přibližně 25 000. Zajímavé je, že všechny výpočty netriviálních nulových bodů až do dnešní doby se provádí právě Turingovou metodou. K dnešnímu dni víme, že Riemannova hypotéza platí pro prvních 10^{13} netriviálních nulových bodů, několik desítek miliard nulových bodů okolo netriviálních nulových bodů řádu 10^{23} a 10^{24} a několik stovek nulových bodů okolo nulových bodů řádu 10^{32}.

Do dnešního dne nebyla Riemannova hypotéza ani potvrzena ani vyvrácena. V každém případě se jedná o jediný problém z 23 matematických problémů vybraných Hilbertem v roce 1900 jako nejzajímavější matematické problémy a jedním ze sedmi, na který vypsal Clayův matematický institut odměnu 1 000 000 amerických dolarů za jeho potvrzení nebo vyvrácení [5]. Aktuálně zbývá pouze šest problémů, protože Poincarého domněnka byla vyřešena. Důkaz podal roku 2003 Grigorij Perelman. Jeho správnost byla potvrzena v srpnu 2006 [12].

4. Po válce

Od roku 1945 byl Turing členem Waltonského atletického klubu, kde se stal brzy nejlepším běžcem. V roce 1947 se účastnil Amatérského atletického maratonského šampionátu a skončil čtvrtý s časem 2:46:03 [1], což bylo pouze o 11 minut více než čas Thomase Richardse na olympiádě v Londýně roku 1948, který zde vybojoval stříbrnou medaili. Dokonce se chtěl zúčastnit olympiády jako maratonský běžec, nebyl však nominován. V roce 1948 pak stříbrného Thomase Richardse porazil v přespolním běhu.

V akademickém roce 1947/1948 se Turing vrátil do Cambridge, kde se zabýval otázkami značně vzdálenými od počítačů nebo matematiky, protože studoval neurologii a fyziologii, přesto byl 4. prosince 1947 přijat Národní fyzikální laboratoří v Teddingtonu, Middlesexu jeho článek *Rounding-off Errors in Matrix Processes* (Zaokrouhlovací chyby v maticových procesech [19]). Rozebírá zde problém zaokrouhlovacích chyb Gaussovy eliminační metody, který se ale týká pouze některých matic [6].

V roce 1948 se Newman stal profesorem matematiky na Univerzitě v Manches-

teru a pozval Turinga, aby zde přednášel. Turing na univerzitě také pracoval společně s F. C. Williamsem a T. Kilburnem na konstrukci počítacího stroje. V roce 1950 na základě zkušeností z této práce publikoval knihu *Computing Machinery and Intelligence in Mind*, ve které si pokládal zásadní otázky týkající se dalšího rozvoje počítačů. Také dlouhodobě uvažoval o možnostech inteligentních strojů a je autorem myšlenky tzv. Turingova testu, která tvrdí, že za inteligentní můžeme stroj považovat tehdy, když nejsme schopni odlišit jeho výstup (například jeho odpovědi) od výstupu člověka [21]. Test definoval následovně:

Představme si tři osoby po řadě označené A, B a C. Osoba A je muž, osoba B je žena a u osoby C není pohlaví relevantní. Osoba C nezná druhé dvě osoby a neví, kdo z nich je A a kdo B – má však za úkol to zjistit. Může oběma klást dotazy, ale pouze takovým způsobem, aby například ze zabarvení hlasu nebylo možné poznat, kdo je muž a kdo žena (nejlépe je představit si, že spolu rozmlouvají přes prostředníka, nebo že si své dotazy a odpovědi píší přes vhodný terminál apod.). Osoba B (žena) se tazateli snaží pomoci, a odpovídá pravdivě. Osoba A (muž) se naopak snaží tazatele zmást, a proto mu může dávat i nesprávné a lživé odpovědi.

Otázka jeho testu pak zní následovně: „Bude-li člověk A nahrazen počítačem, bude tazatel (osoba C) ve svých odpovědích chybovat stejně často, jako když A byl skutečně člověkem?“ V roce 1990 Hugh Loebner založil nadaci, jež prvnímu stroji, který úspěšně složí Turingův test, udělí Loebnerovu cenu a 100 000 amerických dolarů [16]. Do dnešního dne nebyla tato cena udělena.

Po druhé světové válce byly myšlenky Turingova stroje využity při konstrukci prvních počítačů řízených programem uloženým ve vnitřní paměti. V USA a Británii se začala rozvíjet počítačová věda. Turing byl považován za jednu z největších autorit v tomto oboru a jeho teoretické poznatky se v USA začaly zhodnocovat i v praxi. Již v posledních letech války pracovali výzkumníci v USA na konstrukci ENIACu. V roce 1945 vypracoval John von Neumann analýzu logického schématu obdobného zařízení, které mělo být dokonalejší než ENIAC. Von Neumannův článek *První náčrt zprávy o EDVACu* měl obrovský ohlas. Definoval strukturu výpočetních zařízení vůbec, neboť jde o první zevrubné rozpracování ideje programu uchovávaného v paměti. Von Neumann v něm zdůraznil myšlenku, že data i strojové instrukce by se měly ukládat pospolu. Turing, který se po válce stal členem matematického oddělení v Národní fyzikální laboratoři řízené britskou vládou, se s von Neumannovým článkem o EDVACu (Electronic Discrete Variable Automatic Computer) seznámil. Na jeho základě vypracoval vlastní plán velkého počítače nazvaného Automatický počítací stroj (Automatic Computing Engine, ACE) [20], který pak byl také sestrojen, ale prodejně byl neúspěšný. Turing se také podílel na vývoji hardware, programového vybavení a dokumentace [22] počítačů Manchester Mark I a II.

Tyto počítače Turing prakticky využíval v 50. letech, kdy pracoval na teoretickém vysvětlení morfogeneze, což pro něj bylo vlastně luštění kódů života, které jsou založeny na chemické bázi. Na přelomu 40. a 50. let se zaměřil na studium struktury mozku živých bytostí, což bylo poslední téma jeho životní kariéry. Na základě svého studia morfogeneze formuloval jako první matematický popis vzniku nelineárních obrazců (tzv. Turingovy obrazce), což byl jeden z kroků, který později přivedl vědce ke studiu fenoménu samoorganizace a komplexity. V roce 1951 pracoval na aplikaci matematické teorie na biologické formy, kterou se zabýval až do konce svého života.

Napsal pojednání o chemickém základu morfogeneze a předpověděl oscilující chemické reakce, jako je Belousovova–Žabotinského reakce, která byla popsána v roce 1960 [2]. Pokoušel se také vysvětlit výskyt čísel Fibonacciovy posloupnosti v listech rostlin – nejlépe patrné ve spirálách semínek slunečnice nebo jedlových šiškách. Zabýval se také novými myšlenkami kvantové teorie, reprezentací elementárních částic pomocí spinorů a teorií relativity.

V době, kdy se zabýval biologií a morfogenezí, přišel mimo jiné s teorií vysvětlující vznik pravidelných biologických struktur, například tygřích pruhů a dalších vzorů na savčí srsti nebo na ptačím peří. Přemýšlení nad původem vzniku takovýchto struktur ho přivedlo k hypotéze, že jde o výsledek spolupráce dvou biologicky aktivních látek, takzvaných morfogenů. Jeden má aktivační funkci (povzbuzuje například tvorbu tmavého pigmentu), zatím co druhý tento proces blokuje. Spojením jejich vlivu lze vysvětlit střídání tmavých a světlých pruhů na tygří srsti stejně jako vznik jiných pravidelných biologických struktur, což Turing popsal matematickými rovnicemi. V jeho době šlo o teoretický koncept, který neměl žádnou experimentální oporu. Biologové z King's College v roce 2012 v on-line verzi časopisu *Nature Genetics* přinesli první důkaz, že jeho teorie opravdu funguje [8]. Studovali vznik pravidelných prohlubní na horním patře vyvíjejících se myších embryí. Při tom identifikovali dvojici chemických látek, které vznik této struktury řídí. Regulováním jejich aktivity pak dokázali měnit strukturu horního patra způsobem, který přesně odpovídal rovnicím navrženým Turingem.

Za svoji práci o Turingově stroji v roce 1936 se Alan Turing v roce 1951 stal členem Královské společnosti v Londýně.

Alan Turing je i autorem prvního šachového programu TurboChamp. Jednalo se o „papírový" algoritmus, protože Turing následující tah dokázal vypočítat v krátkém čase ručně na papíře. I když v historicky první partii člověka a stroje program prohrál, na to, jak musel být algoritmus výpočetně nenáročný, hrál až neuvěřitelně dobře. K události mělo dojít v roce 1951. Partie (TurboChamp vs. Alick Glennie) měla probíhat takto:

> 1.e4 e5 2.Jc3 Jf6 3.d4 Sb4 4.Jf3 d6 5.Sd2 Jc6 6.d5 Jd4 7.h4 Sg4 8.a4 Jxf3+ 9.gxf3 Sh5 10.Sb5+ c6 11.dxc6 0–0 12.cxb7 Vb8 13.Sa6 Da5 14.De2 Jd7 15.Vg1 Jc5 16.Vg5 Sg6 17.Sb5 Jxb7 18.0-0-0 Jc5 19.Sc6 Vfc8 20.Sd5 Sxc3 21.bxc3 Dxa4 22.Kd2 Je6 23.Vg4 Jd4 24.Dd3 Jb5 25.Sb3 Da6 26.Sc4 Sh5 27.Vg3 Da4 28.Sxb5 Dxb5 29.Dxd6 Vd8 0–1.

Turing se pokoušel svůj program spustit na počítači Mark I na Universitě v Manchesteru, ale neuspěl (neuvádí se, proč přesně, nejspíš program nešel zkompilovat).

Alan Turing se v roce 1941 zasnoubil se svou kolegyní Joan Clarke z Bletchley Parku. Toto zasnoubení však zrušil brzy poté, co jí pověděl o své homosexualitě. V roce 1952 se v souvislosti s krádeží v Turingově domě policie dověděla o jeho vztahu s devatenáctiletým Arnoldem Murrayem z Manchesteru. Takové jednání bylo ve Velké Británii až do roku 1994 trestné. V souvislosti s tím mu byla zrušena bezpečnostní prověrka a skončila tedy i jeho práce pro Vládní komunikační centrum GCHQ. Mohl sice dále přednášet, ale myšlenka, že by mohl začít spolupracovat s von Neumannem, se rozplynula, neboť nedostal vízum do USA. Turing představoval pro britskou bezpečnostní službu vážné nebezpečí, protože měl řadu zahraničních kolegů po celém světě. Policie začala tajně sledovat jeho zahraniční návštěvy.

Turing byl zatčen a 31. března 1952 odsouzen a musel volit mezi ročním vězením a probací – podmíněným prominutím trestu, které ovšem bylo vázáno na podstoupení roční hormonální „léčby“ (organo-therapic treatment). Rozhodl se pro druhou možnost a po dobu jednoho roku dostával ke snížení libida dávky estrogenu. Fakticky se jednalo o chemickou kastraci. Estrogen navíc běžně způsoboval gynekomastii (růst prsů), což je nevítaný příklad morfogeneze, kterou se zrovna zabýval.

V roce 1953 odjel na dovolenou do Řecka, což vyvolalo v bezpečnostní službě značné znepokojení. To je také důvod, proč někteří autoři mluví o Turingově smrti spíše jako o vraždě na vládní příkaz než o sebevraždě.

Dne 7. června 1954 Turing zemřel na otravu kyanidem draselným. Tím mělo být napuštěno jablko, kterého několik soust snědl. Přítomnost kyanidu v jablku však nebyla testována. Jako příčina smrti byl kyanid určen až při pitvě. Podle oficiálního stanoviska se jednalo o sebevraždu, čímž byly odmítnuty spekulace o náhodě (nedbalé skladování chemikálií), nebo o vraždě (politické, špionážní).

5. Současnost

Na počest Alana Turinga je od roku 1966 udílena Turingova cena, jedno z nejvýznamnějších informatických ocenění. V roce 1999 časopis *Time* označil Turinga jako jednoho ze 100 nejdůležitějších lidí 20. století za jeho přínos k rozvoji umělé inteligence a moderních počítačů. V roce 2007 byla zhotovena plně funkční replika počítače Colossus Mark 2 pod vedením Tonyho Salea.

V září 2009 se britský premiér Gordon Brown jménem vlády omluvil Alanu Turingovi za příkoří, které mu bylo způsobeno, když byl odsouzen pro homosexualitu. Omluvu zveřejnil list *The Daily Telegraph*. „Jménem britské vlády a všech těch, kdo díky Alanově práci žijí svobodně, říkám: Je nám to líto. Zasloužil jste si něco lepšího,“ napsal Brown. „Není přehnané říci, že bez jeho mimořádného přispění mohly být dějiny druhé světové války velice odlišné. To, za co mu musíme být vděčni, staví do ještě hroznějšího světla fakt, že se s ním jednalo tak nelidsky“ [4].

V prosinci 2011 byla na webové stránce Direct Gov vytvořena petice, která žádala, aby byl Turing omilostněn. Získala více než čtyřiatřicet tisíc podpisů, ale lord McNally, tehdejší tajemník ministerstva spravedlnosti, se jí odmítl zabývat a řekl, že Turing byl „náležitě odsouzen“ za něco, co bylo tehdy trestným činem. Veřejná kampaň za Turingovo očištění trvala roky a podporovaly ji osobnosti jako bývalý britský premiér Gordon Brown nebo slavný vědec Stephen Hawking.

Dne 23. června 2012 uplynulo 100 let od Turingova narození. Na Univerzitě v Manchesteru se pořádala na jeho počest konference, kde se při této příležitosti objevila celá řada osobností světa IT, např. David Ferrucci z IBM nebo „otec internetu“ Vint Cerf. Při této příležitosti Turingův šachový algoritmus TurboChamp sehrál další partii, tentokrát běžel na počítači. Proti programu usedl nejlepší lidský šachista dosavadní historie Garry Kasparov (jehož prohra s počítačem Deep Blue v roce 1997 byla dalším milníkem v historii počítačového šachu). Garry Kasparov snadno zvítězil. *The Register* s dalším odkazem na Turinga poznamenává, že Kasparov lidské hráče vesměs snadno poráží a v tomto smyslu TurboChamp vlastně úspěšně složil Turingův test inteligence.

Dne 24. prosince 2013 byla Alanu Turingovi konečně udělena královská milost. Byl tím zbaven všech obvinění. Milost se většinou v Británii uděluje, pouze když se

obvinění ukáže jako falešné, nebo pokud o milost požádá rodina na základě nevinnosti pachatele. Třetí možností je žádost ministra spravedlnosti. „Doktor Alan Turing byl mimořádný muž s mimořádnou myslí. Jeho genialita pomohla ukončit válku a zachránila tisíce životů. Jeho pozdější život byl zastíněn jeho odsouzením za homosexualitu. Tento rozsudek bychom nyní považovali za nespravedlivý a diskriminační, a proto byl rozsudek odvolán. Turing si zaslouží být uznáván za své přínosy ve válečném tažení a ve vědě o počítačích. Milost od královny je adekvátní hold tomuto skvělému muži," řekl k milosti ministr spravedlnosti Velké Británie Chris Grayling [13]. P. Tatchell řekl, že by rád viděl plné vyšetření Turingovy smrti. Prohlásil: „Přestože nemám žádný důkaz, že byl zavražděn, myslím si, že musíme prozkoumat možnost, že mohl být zabit bezpečnostními službami. Bylo na něj nahlíženo jako na velké bezpečnostní riziko."

Glyn Hughes, tvůrce památníku Alana Turinga v Manchesteru, považuje za „velmi potěšující", že mu byla konečně udělena milost. „Když jsme začali se snahou učinit ho slavným, zajistit uznání, bylo velmi složité sehnat peníze," řekl. „Žádná z velkých počítačových firem nechtěla na jeho památník přispět ani penny. Teď by to možná udělaly."

6. Životopis

1912 (23. června): Narozen v Paddingtonu, Londýn
1926–31: Střední škola Sherborne
1930: Smrt jeho přítele Christophera Morcoma
1931–34: Studium na King's College, Univerzita v Cambridge
1932–35: Studium v oblasti kvantové mechaniky, pravděpodobnosti a logiky
1935: Zvolen členem univerzitní koleje King's College v Cambridge
1936: Turingův stroj, teoretický model univerzálního výpočetního stroje
1936–38: Universita v Princetonu. Obhájil doktorát z logiky, studium algebry a teorie čísel
1938–39: Návrat do Cambridge. Počátek kryptoanalýzy Enigmy
1939–40: Bomba, stroj na dešifrování Enigmy
1939–42: Prolomení námořní verze kódu Enigma, tím došlo ke zlomu v bitvě o Atlantik
1943–45: Hlavním konzultantem pro kryptoanalýzu. Práce na elektronických počítačích
1945: National Physical Laboratory v Londýně
1946: Návrhy počítačů a software
1947–48: Programování, neuronové sítě, umělá inteligence
1948: Univerzita v Manchesteru
1949: První skutečné použití počítačů v matematice, Manchester Mark I
1950: Turingův test umělé inteligence
1951: Zvolen členem Královské společnosti. Nelineární teorie biologického růstu
1952: Obvinění z homosexuality, ztráta bezpečnostní prověrky
1953-54: Nedokončená práce z biologie a fyziky, morfogeneze
1954 (7. června): Smrt (pravděpodobně sebevražda) otravou kyanidem, Wilmslow, Cheshire

[1] Athletics: marathon and decathlon championships. The Times, 25. 8. 1947.

[2] Belousov–Zhabotinsky reaction. Wikipedia. Online dostupné z: http://en.wikipedia.org/wiki/Belousov%E2%80%93Zhabotinsky_reaction

[3] Bieliková, M., Friedrich, G., Gottlob, G., Katzenbeisser, S., Turán, G.: *The legacy of Turing in numerical analysis*. SOFSEM 2012: Theory and Practice of Computer Science, Springer, Berlin–Heidelberg, 2012.

[4] Brown, G.: *I'm proud to say sorry to a real war hero*. The Telegraph, 2009 [online]. Dostupné z: http://www.telegraph.co.uk/news/politics/gordon-brown/6170112/Gordon-Brown-Im-proud-to-say-sorry-to-a-real-war-hero.html

[5] Derbyshire, J.: *Posedlost prvočísly*. Academia, 2007.

[6] Dopico, F. M.: *Alan Turing and the origins of modern Gaussian elimination*. Instituto de Ciencias Matemáticas, 2010 [online]. Dostupné z: http://gauss.uc3m.es/web/personal_web/fdopico/papers/arbor-2011-turing.pdf

[7] Durnová, H.: *Alan M. Turing (1912–1954): Matematika, programování a umělá inteligence*. PMFA *57* (2012), 339–342. Online dostupné z: http://dml.cz/bitstream/handle/10338.dmlcz/143219/PokrokyMFA_57-2012-4_9.pdf

[8] Green, J. B. A., et al.: *Periodic stripe formation by a Turing mechanism operating at growth zones in the mammalian palate*. Nature Genetics (2012), doi:10.1038/ng.1090.

[9] Hejhal, D. A., Andrew, M., Odlyzsko, A. M.: *Alan Turing and the Riemann zeta function*. Elsevier, 2011.

[10] Hodges, A.: *Alan Turing: the Enigma* [online]. Dostupné z: http://www.turing.org.uk/

[11] Hodges, A.: *Alan Turing: one of the great philosophers* [online]. Dostupné z: http://www.turing.org.uk/publications/philobook.html

[12] Problémy tisíciletí (Millenium Prize Problems). Wikipedia. Online dostupné z: http://cs.wikipedia.org/wiki/Probl%C3%A9my_tis%C3%ADcilet%C3%AD

[13] Royal pardon for codebreaker Alan Turing. BBC 24. 12. 2013. Online dostupné z: http://www.bbc.com/news/technology-25495315

[14] Singh, S.: *Kniha kódů a šifer*. Dokořán a Argo, 2009.

[15] The imitation game [online]. Dostupné z: http://www.imdb.com/title/tt2084970

[16] The Loebner prize in artificial intelligence. Online dostupné z: http://www.loebner.net/Prizef/loebner-prize.html

[17] Turing, A.: *On computable numbers, with an application to the Entscheidungsproblem*, 1937. Online dostupné z: http://www.turingarchive.org/browse.php/B/12

[18] Turing, A.: *A method for the calculation of the zeta-function*. London Mathematical Society, 1943. Online dostupné z: http://www.turingarchive.org/browse.php/B/17

[19] Turing, A.: *Rounding-off errors in matrix processes*. National Physical Laboratory, Teddington, Middlesex, 1947. Online dostupné z: http://qjmam.oxfordjournals.org/

[20] Turing, A.: *ACE (Automatic Computing Engine)*. Poznámky k přednášce, 1947. Online dostupné z: http://www.turingarchive.org/browse.php/B/1

[21] Turing, A.: *Can digital computers think?* Poznámky k rozhovoru BBC, třetí program, 15. 5. 1951. Online dostupné z: http://www.turingarchive.org/browse.php/B/5

[22] Turing, A.: *Programmers' handbook for Manchester electronic computer Mark II, with errata sheets*, 1951. Online dostupné z: http://www.turingarchive.org/browse.php/B/32