June 14th

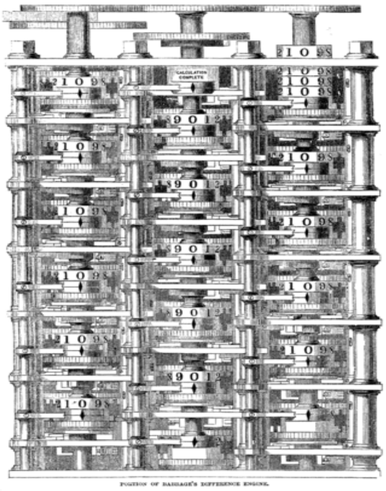
Difference Engines

June 14, 1822

Charles Babbage [Dec 26] probably began designing his first Difference Engine in 1819. The principal aim was to employ Newton’s method of divided differences to calculate mathematical tables, a task currently carried out by unreliable human “computers”.

On this day, Babbage announced the prototype’s completion in a paper entitled, “Note on the application of machinery to the computation of astronomical and mathematical tables,” which he presented at the Royal Astronomical Society in London. He also wrote to Humphry Davy on [July 3], 1822 giving an expanded description of the device.

The British government's interest was piqued, and it granted Babbage £1700 in 1823 to build a complete version. Babbage brought in engineer Joseph Clement to implement his revised design, and (after much squabbling) they eventually produced a model utilizing around 1/7 of the proposed calculating unit.



Part of the Difference Engine No. 1. Drawing by Benjamin Herschel Babbage (1864).

By the mid-1830's, Babbage seems to have lost interest in the Difference Engine as he concentrated on the more ambitious Analytical Engine [Dec 23], although he occasionally dabbled, producing a Difference Engine No 2 design in the late 1840's. Inevitably, the government stopped funding the project, having handed over £17,000 without receiving anything close to a working device.

Although Babbage never finished an engine (Difference or Analytical), Per George Scheutz [Sept 23] did complete a machine based on Babbage's early Difference Engine designs in 1854.

A Difference Engine No. 2 finally ran on [Dec 26] 1991, proving that Babbage’s later plans were implementable.

Alonzo Church

Born: June 14, 1903;

Washington, DC
Died: Aug. 11, 1995

Church made major contributions to mathematical logic, recursion theory, and theoretical computer science.

In 1936 he published Church’s Theorem, which considered the Entscheidungsproblem (“Decision Problem” in German), as to whether there is a general procedure to determine the truth of any first-order logic statement. His theorem showed that no such algorithm existed.

Church was heavily influenced by Kurt Gödel’s [April 28] earlier incompleteness theorem, especially by his method of assigning numbers (now known as Gödel numbering) to logical formulas to reduce them down to arithmetic.

Church's work completed the answer to David Hilbert’s second problem [Sept 3]: is mathematics complete, is it consistent, and is it decidable? In 1931, the first two parts had been answered in the negative by Gödel, and Church had now added “no” for decidability.

Church's proof utilized his lambda calculus which defines computation in terms of functions and how they are simplified (reduced). The Church–Rosser theorem states that the ordering in which reductions are carried out doesn't affect the eventual result.

Church’s Theorem was presented to the American Mathematical Society on April 19, 1935 and published on April 15, 1936, which meant that it predated Turing’s paper [Nov 12] on the Entscheidungsproblem. Turing came to the same negative conclusion about decidability, but by utilizing his Turing machine.

Church and Turing set about combining their approaches, and the resulting Church-Turing thesis states that a function on the natural numbers is computable in an informal sense (e.g., solvable by a human using pencil-and-paper) if and only if it is computable by a Turing machine. Also, the lambda calculus, the Turing machine, and general recursive functions all have the same expressive power (i.e. they can be used to implement the same computable functions).

Lambda calculus later inspired John McCarthy’s [Sept 4] LISP language, and the first report on LISP was published on the same day as Church’s Theorem paper, but 23 years later, on [April 15] 1959.

Church was known for speaking slowly, with an emphasis on forming sentences with a clear logical structure, For example, he would not say: “It is raining”, but might instead declare: " I must postpone my departure inasmuch as it is raining, a fact which I can verify by looking out of the window."

Brijendra Kumar Syngal

Born: June 14, 1940;

Ambala, Punjab, India
Died: 9 July, 2022

Syngal is often called the ‘Father of Internet & Data Services in India’. Under his chairmanship (1991-1998), VSNL (Videsh Sanchar Nigam Limited), India’s leading telecommunication provider, launched the country's first publicly-available Internet service in five cities (Delhi, Bombay, Kolkata (then Calcutta), Chennai (then Madras) and Pune) on 15 August 1995.

Newspapers gleefully called it India's "Second Independence Day", but the euphoria quickly turned sour.

Customers trying to access the internet from cities outside the chosen five had to make long-distance calls at a prohibitive 35 rupees a minute. Individuals had to cough up an eye-watering 15,000 rupees for an account, while businesses had to pay 25,000 rupees.

There were so many technical glitches that within a month questions were being raised in Parliament. Syngal called a press conference and announced: “I goofed up. Give me ten weeks and you’ll get a system that India will be proud of.”

He fulfilled that promise by adding more servers, getting the phone department to improve connectivity, moving from copper to fiber-based cables, by slashing the tariffs by half, and by encouraging private firms to sell internet services.

In 1998, he was named one of the '50 stars of Asia' by *Business Week* . Unofficially, he was also known as ‘Bulldozer’, for his ability to crash through bureaucratic barriers.

A Plankalkül Draft

June 14, 1945

The earliest surviving draft of Konrad Zuse's [June 22] Plankalkül, the first high-level programming language, bears today's date. However, notes referring to Plankalkül date back to May 1939, and it's known that Zuse wrote a chess program in the language in 1942, which preceded Claude Shannon’s article about computer chess [Nov 8], and Turing and Champernowne's Turochamp [June 25] by several years.

Zuse used Plankalkül in his doctoral dissertation which was completed in late 1945, but wasn’t widely available until 1972.

The first published paper about Plankalkül appeared in the German journal *Archiv der Mathematik* in 1948 but didn’t attract much attention. In the same year Zuse also presented the language at the Annual Meeting of the GAMM, a German science society,

The fact that the language was designed in Germany during WWII meant that it was isolated from developments in England and the US. Nevertheless, it pioneered many features from later languages, including assignment, conditionals, iteration, subroutines, floating point arithmetic, arrays, records, assertions, and exception handling.

Plankalkül programs were laid out in a novel two-dimensional form, somewhat suggestive of a spreadsheet.

$$\begin{array}{c|ll} & R(V) & \Rightarrow R \\ V & 0 & 0 \\ S & m\times\sigma & m\times\sigma \end{array}$$

$$\begin{array}{c|ll} & W1(m) & \left[\begin{array}{ll} V \Rightarrow R & \\ 0 & 0 \\ i & m-1-i \\ \sigma & \sigma \end{array}\right] \\ V & & \\ K & & \\ S & & \end{array}$$

Converting an array to a list. From Konrad Zuse's Thesis (1945).

In the late 1950's, Zuse was unhappy that the designers of ALGOL 58 [May 27] didn't acknowledge Plankalkül, even though many of them were aware of it.

The first Plankalkül compiler was implemented in 1975 by Joachim Hohmann.

Robert M. Frankston

Born: June 14, 1949;

Brooklyn, New York

Frankston is the co-creator with Dan Bricklin [July 16] of VisiCalc [May 11] [Oct 19] , and the co-founder of Software Arts [Jan 2], the company that published it.

Although Bricklin came up with the spreadsheet concept, it was Frankston that implemented the first commercial version, initially for the Apple II [June 5]. He coded in 6502 assembler via an account on MIT’s Multics System [Nov 30], which he logged into from his attic apartment in Arlington. He then downloaded the software over a phone line to test it on an Apple II.

Frankston was very familiar with the 6502, having written an extended BASIC for a 6502 microprocessor the previous year. He and Bricklin were also knowledgeable about Multics as they’d worked on it together while undergraduates at MIT.

Frankston was one of the founders of the MIT Student Information Processing Board, a time-sharing project that gave non-computing students access to computers.

At his mother’s insistence, the family name had been changed from Frankenstein to Frankston. Frankston later explained, “You can imagine my uncle Boris trying to sell life insurance.”

Aspen Movie Map

July 14-18, 1980

The Aspen Movie Map was an early hypermedia system (created between 1978-1980) that allowed users to interactively explore and navigate the roads of Aspen, Colorado. Andrew Lippman, the project's director, gave a talk about the work on this day at SIGGRAPH 80, entitled "Movie-maps: An application of the optical videodisc to computer graphics."

In 1978 the Architecture Machine Group at MIT was given one of the first laserdisc [Dec 11] players by MCA . Instead of using it to simply store and playback movies, they'd added interactive controls, including a touch screen display.

Filming for the Aspen project was carried out by mounting a gyroscopic stabilizer on top of a car, which could carry several 16mm stop-frame cameras with wide-angle lenses. A fifth wheel added to the vehicle triggered the cameras every 10 feet.

Photography took place daily between 10am and 2pm to minimize any lighting discrepancies between different shoots. Also, the car drove down the center of the streets to make it easier to stitch different pieces of film together. Thousands of still frames, audio, and other data were collected.

In 1980 the Aspen Movie Map was awarded a "Golden Fleece Award" by US Senator William Proxmire, a sarcastic award he bestowed on projects which he deemed wastes of taxpayer money. Of course, the core ideas of the project have since become ubiquitous, most notably in Google Street View [May 14].

For more maps, see [Feb 4], [Feb 8], [March 6], [Aug 9], [Sept 19], [Dec 24].

Novell Buys UNIX, Sells, then Buys

June 14, 1993

Novell announced the completion of its acquisition of UNIX System Labs from AT&T. An event that was later seen as a major turning point in the so-called UNIX wars [Feb 14].

Ray Noorda [June 19], Novell's co-founder, chairman and CEO, wanted to use UNIX to extend the company's NetWare enterprise services, and the company subsequently released UnixWare, which essentially merged NetWare with UNIX System V Release 4.

Dennis Ritchie [Sept 9] likened the UNIX System Labs sale to the Biblical story of Esau (Genesis 25:29-34) selling his birthright for a mess of pottage (lentil stew).

Noorda was replaced by Robert Frankenberg in 1994, and soon after Novell sold off portions of its UNIX business to the Santa Cruz Operation (SCO) [Jan 00]. Whether Novell also sold the copyright to UNIX and UnixWare would later become the subject of some intense litigation [Aug 10].

Meanwhile, newer OSes, such as Windows 95 [Aug 24], Linux [March 14], and OS/2 [Oct 11], now included their own network functionality, which greatly reduced demand for third-party products. As a consequence, there was a steep decline in Novell's market share

Just over ten years later (on Nov. 4, 2003), Novell announced that it was buying SuSE Linux. This was possible since IBM had just bought $50 million worth of Novell's stock.

Flying Toasters Sued

June 14, 1994

The screensaver software, After Dark, was written by Jack Eastman and Patrick Beard, and sold by Berkeley Systems. Version 1.0 from 1989 featured rather boring line art: water ripples, worms, rainfall, and stars, but After Dark 2.0, released in March 1992, triggered the screensaver boom of the 1990's.

The most famous of its modules was "Flying Toasters", which featured 1940's-style chrome toasters with wings flying across the screen. A slider enabled users to adjust the toast's darkness, and a later version added a choice of music, including Richard Wagner's "Ride of the Valkyries". Apparently, Eastman got the idea while wandering around the house, half asleep, and noticed the toaster in the kitchen.

A Non-flying Toaster. Photo by Peng. CC BY-SA 3.0.

After Dark version 2 also supported third-party modules, a canny move since it encouraged users to contribute many hundreds, which bolstered the product's popularity.

But not everything was peachy. The rock group "Jefferson Airplane" filed a lawsuit on this day, claiming that After Dark's toasters were a copy of the winged toasters featured on the cover of their 1973 album "Thirty Seconds Over Winterland". However, the case was eventually dismissed because the art hadn't been registered as a trademark.

Ironically, that lawsuit had been triggered by Berkeley Systems suing another company in Sept. 1993 over its "Death Toasters" screensaver, in which Opus (of "Bloom County" fame) fires a shotgun at passing toasters.

LOLCATS Can Haz Domain

June 14, 2006

A lolcat is an image of one or more cats, often accompanied by grammatically incorrect text, known as lolspeak. The "lol" part comes from the abbreviation LOL (laugh out loud).

The term "lolcat" probably originated on 4chan [Oct 1], and the domain name LOLcats.com was registered on this day.

Of course, amusing cat pictures have a much longer history. For example, in the early 1870's, British portrait photographer Harry Pointer specialized in carte de visite (visiting cards) featuring cats in funny poses, which he often augmented with jocular textual comments.

In 2007, Adam Lindsay created LOLCODE, an esoteric programming language [May 26], based on lolspeak.

Hertzbleed Disclosed

June 14, 2022

Hertzbleed is a hardware security attack which exploits dynamic frequency scaling, a kind of timing attack, to reveal secret data.

Dynamic frequency scaling changes the CPU's frequency to maintain power consumption and temperature constraints. Since power consumption depends on the data being processed, a remote attacker can deduce the data from the CPU's overall execution time.

For example, the calculation 2022 + 23823 compared to 2022 + 24436 may run at a different CPU frequency, and therefore take a different amount of time to complete.

Hertzbleed is classified as a *side-channel attack*: an exploit based on extra information that can be gathered because of the fundamental way a protocol or algorithm is implemented, rather than flaws in the design of the protocol or algorithm itself.

A recently declassified NSA document reveals that as far back as 1943, an engineer with Bell telephone observed decipherable spikes on an oscilloscope associated with the decrypted output of a certain encrypting teletype. For another example, see [July 23].