A Lehmer szita

Szalkai István, 2019

Derrick Norman Lehmer

(1867 – 1938)
amerikai

Derrick Henry Lehmer

(1905 – 1991)
amerikai

D.N.Lehmer (id.) Prímszám táblázatok és faktorizációk 10,017,000 –ig (1909).

Apa és fia:

Elektro (csak kapcsolók) -mechanikus eszközök a prím-faktorizációra:

1926: *bicikli láncokból* (3 mp)

$2^{93} + 1 = 3*3 * 529\,510\,939 * 715\,827\,883 * 2\,903\,110\,321$

1932: fogaskerekekből (5000 eset /mp)

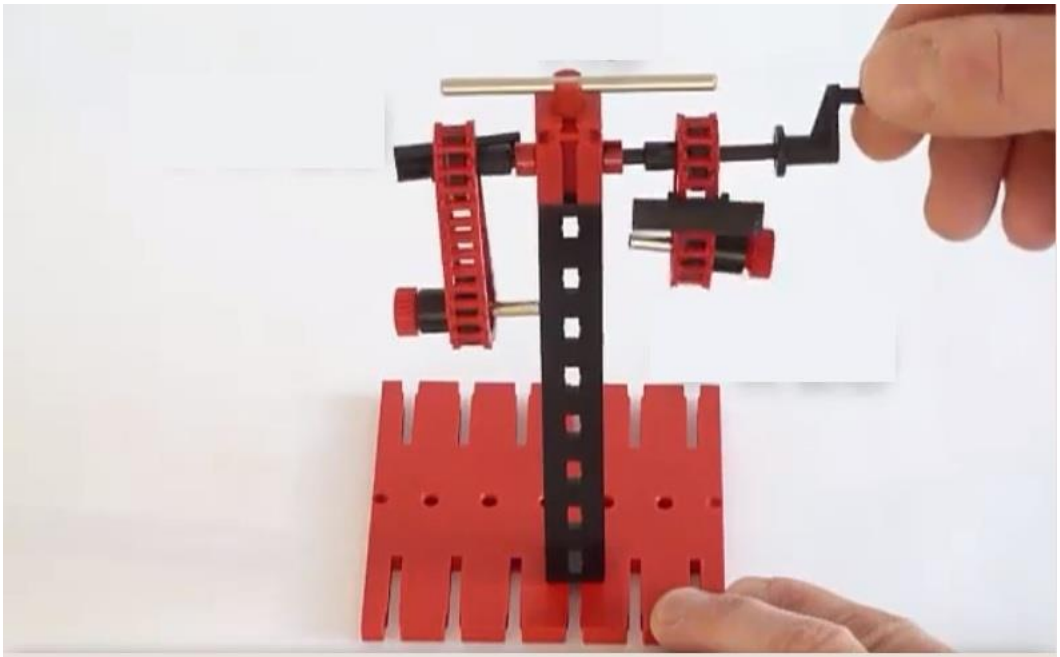
1936: 16 mm film

Hasonló elv IC –kben

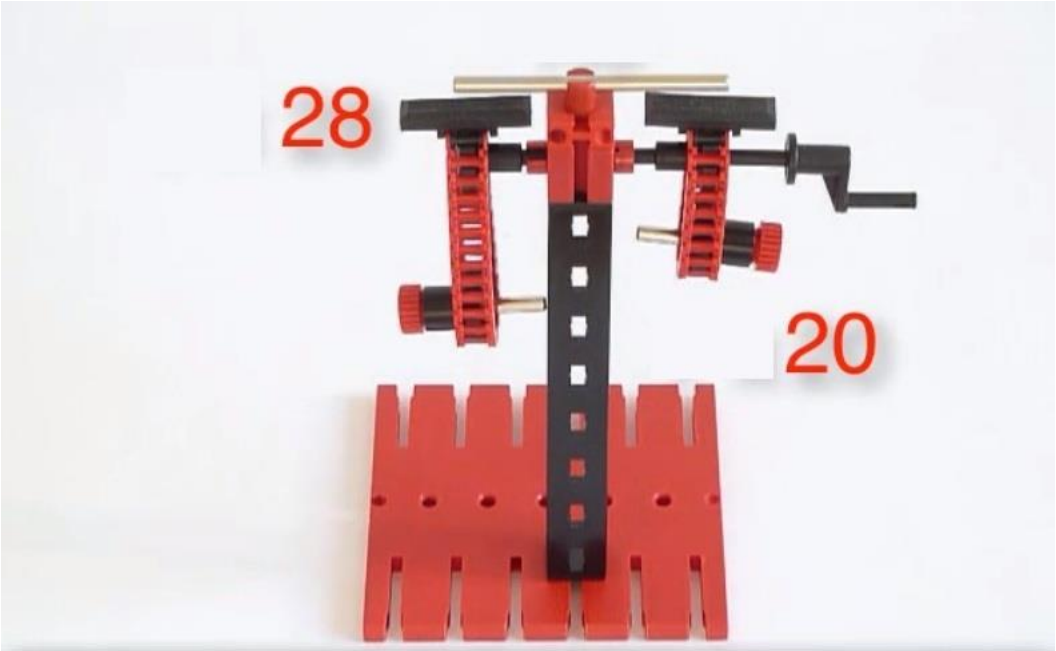

COMPUTER
HISTORY
MUSEUM


COMPUTER
HISTORY
MUSEUM

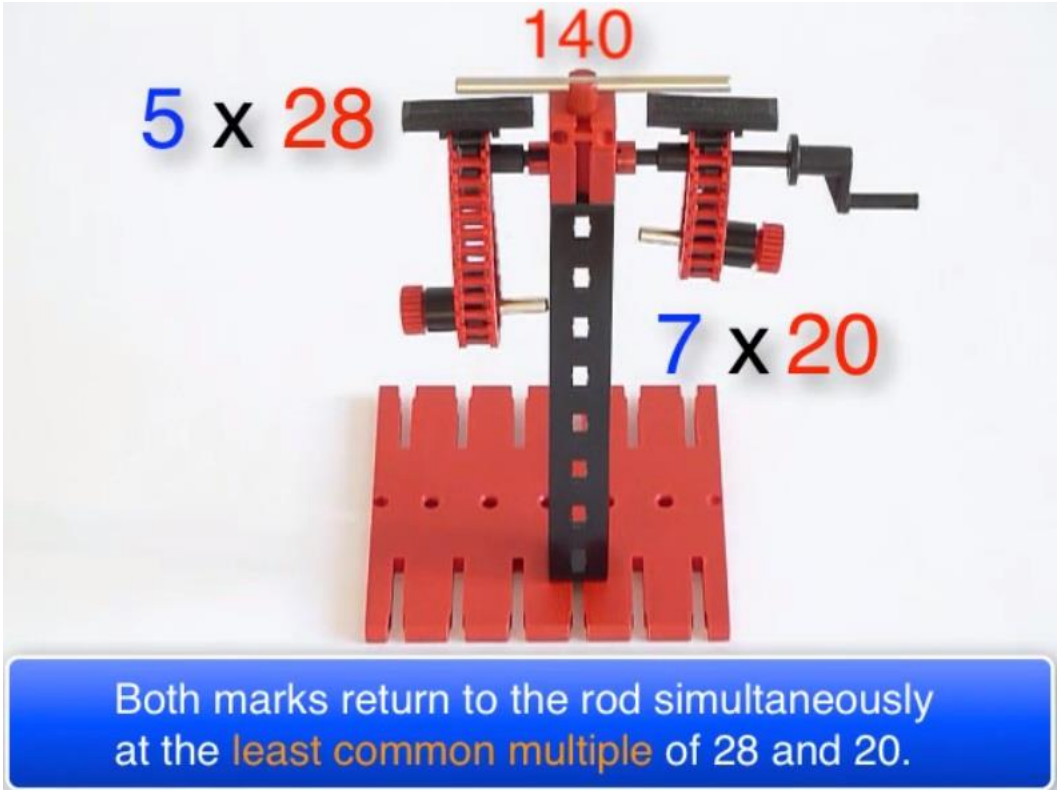

COMPUTER
HISTORY
MUSEUM



https://www.youtube.com/watch?v=Jmncvzo_VMc



https://www.youtube.com/watch?v=Jmncvzo_VMc


140
5 x 28
7 x 20
Both marks return to the rod simultaneously
at the least common multiple of 28 and 20.

A Mersenne számok Lucas-Lehmer **prímtesztje:**

HA $p \in \mathrm{P}$ prím, akkor

$$M_p := 2^p - 1 \quad \text{prím} \quad \Leftrightarrow \quad M_p \mid a_{p-1}$$

ahol $a_1 = 4$ és $a_{n+1} \equiv (a_n)^2 \pmod{M_p}$. □

Megjegyzés: (mod M_p) lényeges!

Marin Mersenne (1588 - 1648) francia
François Édouard Anatole Lucas (1842 - 1891) francia

(Ál-) véletlenszám generátor:

Ha X_0 relatív prím m –hez, a rendje nagy ($a^i \neq 1 \pmod{m}$) , akkor legyen

$$X_{k+1} \equiv a \cdot X_k \pmod{m} \; .$$ □

Megjegyzés: determinisztikus!

Más néven: **Park–Miller** véletlenszám generátor.

Gyorsított Euklideszi algoritmus.

Euklidesz (Kr.e. IV.kp. - III.kp.) görög

Gyorsított Euklideszi algoritmus.

Euklidesz (Kr.e. IV.kp. - III.kp.) görög

Irodalom:

https://en.wikipedia.org/wiki/Derrick_Norman_Lehmer

https://en.wikipedia.org/wiki/Lehmer_sieve

https://en.wikipedia.org/wiki/Derrick_Henry_Lehmer

https://en.wikipedia.org/wiki/Édouard_Lucas

https://en.wikipedia.org/wiki/Marin_Mersenne

https://en.wikipedia.org/wiki/Lucas-Lehmer_test

http://ed-thelen.org/comp-hist/Lehmer-NS03.html

http://ed-thelen.org/comp-hist/Lehmer-NS-01.html

http://ed-thelen.org/comp-hist/Mike-Williams-Lehmer.html

https://www.youtube.com/watch?v=Jmncvzo_VMc

https://hu.wikipedia.org/wiki/Mersenne-prímek

https://en.wikipedia.org/wiki/Lucas-Lehmer_primality_test

http://www.computerhistory.org/visiblestorage/ancient-1940s/precomputing/mechanical-devices/

Köszönöm a figyelmet !