Lukuteoria 1 1.2.2022

$p \in \mathbb{N} - \{0,1\}$ on **alkuluku**, jos p:n pos. tekijät ovat 1 ja p. muuten yhd. luku

Eukleides: Alkulukuja on ∞ monta

APL: Jos $n \in \mathbb{N} - \{0,1\}$, niin (sillä on) alkutekijäesitys $n = p_1^{e_1} \cdots p_r^{e_r}$, missä $p_1, \ldots, p_r$ alkulukuja, $e_1, \ldots, e_r \in \mathbb{N} - \{0\}$. Esitys on 1-käsitteinen, jos alkuluvut otetaan suuruusjärjestyksessä.

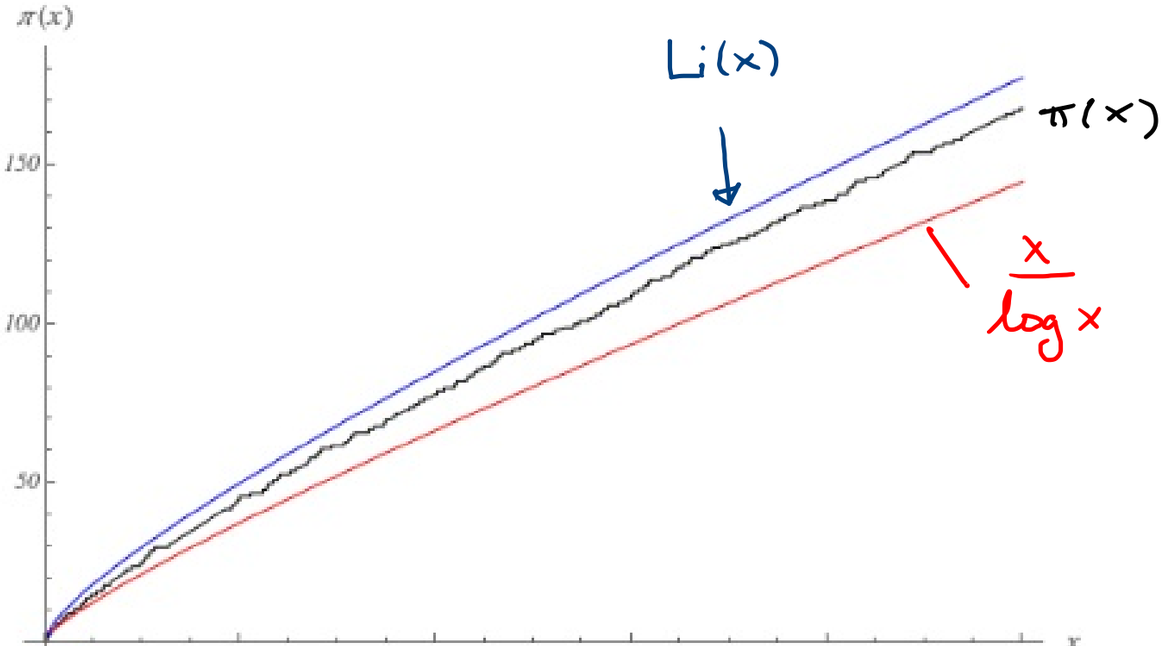
Alkulukuja 2, 3, 5, 7, 11, 13, ...

Kuinka "tiheässä" alkuluvut ovat?

$\pi : [0, \infty[\longrightarrow \mathbb{N}$, $\pi(x) = \#\{p : p \text{ alkuluku}, p \leq x\}$.

x	1	2	3	4	5	6	7	8	9	10	11
$\pi(x)$	0	1	2	2	3	3	4	4	4	4	5

log = luonn. logaritmi.



Li(x)

π(x)

$\frac{x}{\log x}$

Li on logaritmin integraalifunktio

$$Li(x) = \int_2^x \frac{1}{\log t}\, dt$$

$x \geq 2$.

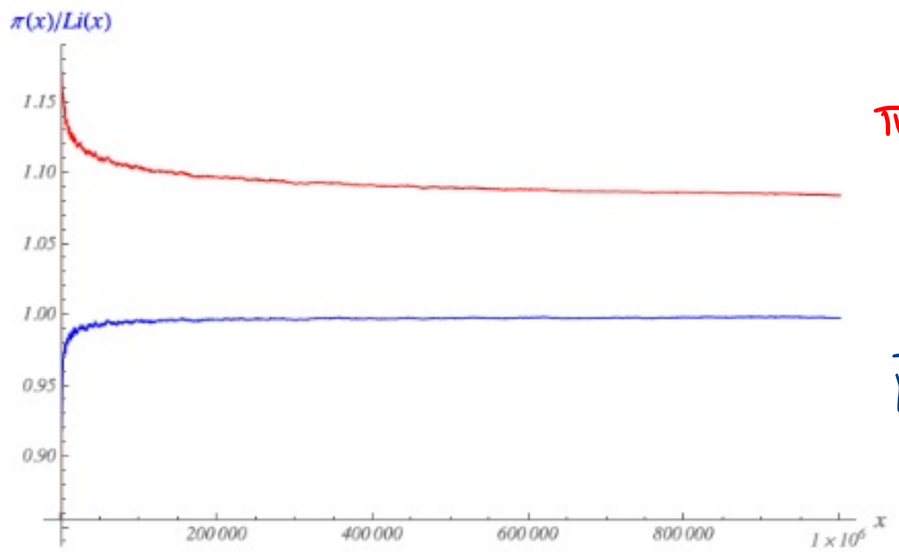
Alkulukulause (Hadamard, de la Vallée Poussin)

Suurilla x pätee

$$\pi(x) \sim \frac{x}{\log x}$$

$$\pi(x) \cdot \frac{\log x}{x} \xrightarrow{x\to\infty} 1$$

$$\frac{\pi(x)}{Li(x)} \xrightarrow{x\to\infty} 1$$



$\pi(x) \cdot \frac{\log x}{x}$

$\frac{\pi(x)}{Li(x)}$

Alkulukujen tiheys välillä $[0, x]$ = $\frac{\pi(x)}{x} \sim$ alkul. lause $\frac{x/\log x}{x} = \frac{1}{\log x} \xrightarrow[x\to\infty]{} 0$

Sunnilla luvuilla alkuluvut ovat harvassa.

x	10	100	1000	10000	100000	10^6	$\cdots$	10^{13}
$\pi(x)$	4	25	168	1229	9592	78498	$\cdots$	346065536839
$\frac{\pi(x)}{x}$	0.4	0.25	0.17	0.12	0,096	0.078	$\cdots$	0.035

$a, b \in \mathbb{Z}$, $c_k^{a,b} = a + kb$

$(c_k^{a,b})_{k=0}^{\infty}$ on aritmeettinen jono

Dirichlet'n lause alkuluvuista aritmeettisissa jonoissa

Jos $a > 0$, syt $(a, b) = 1$, niin jonossa $(c_k^{a,b})_{k=0}^{\infty}$ on ∞ monta alkulukua.

Esim. 1) $a = 1$, $b = 2$ } — parittomat luonn. luvut.
$c_k^{1,2} = 1 + 2k$
Eukl. lause: alkulukuja on ∞ monta
2 on ainoa parillinen alkuluku ⇒ parittomia alkulukuja on ∞ monta.

1, 3, 5, 7, 9, 11, 13, 15, 17, ...

2) $a=1, b=4$: 1 5 9 13 17 21 25 29 33 37 41

($a=2, b=4$ syt $(2,4)=2$ kaikki parillisia luonnollisia luku 2 on aina jonossa $(c_k^{2,4})_{k=0}^{\infty}$ oleva alkuluku)

$a=3, b=4$ 3 7 11 15 19 23 27 31 35 39 43

Huom: $a=5, b=6$

Lause Muotoa $4n+3$ olevia alkulukuja on ääretön määrä.

Tod. Olk. $p_1, \dots, p_k$ alkulukuja, jotka ovat muotoa $4n+3$. $p_i \neq 3$

Huom. tällaisia on: 3, 7, 11, 19 jne. Olk.

$N = 4p_1 \cdots p_k + 3$.

Jos N on alkuluku, niin $N > p_i$ kaikilla $1 \le i \le k$ $\rightsquigarrow$ löydettiin uusi alkuluku, joka on haluttua muotoa

Ol. että N ei ole alkuluku.

Huom $p_i \mid 4p_1 \cdots p_k$, $p_i \nmid 3$ $\Rightarrow$ $p_i \nmid N$ ($2 \mid 4p_1 \cdots p_k$, $2 \nmid 3$ $\Rightarrow$ $2 \nmid N$)

Lause 3.10 APL : $N = q_1 \cdots q_s$, missä $q_1, \dots, q_s$ alkulukuja.

Jaakoyhtälö: $q_i = 4n_i + r_i$, $0 \le r_i \le 3$

Huom. 1) $r_i \neq 0$, koska $4n_i$ ei ole alkuluku.

$\neq 2$, koska $4n_i + 2 = 2(n_i + 1)$ jos $2 \nmid N$.

$\Rightarrow r_i \in \{1, 3\}$.

2) $(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1$

Jos kaikki q_i:t olisivat muotoa $4n+1$, niin $q_1 \cdots q_s = 4M+1$

Mutta tämä on mahdotonta, koska $N = 4p_1 \cdots p_k + 3$

Siis ainakin yksi luvuista q_i on haluttua muotoa $4n+3$.

Huom. $3 \mid 3$

$3 \nmid 4p_1 \cdots p_k$, koska muuten jokin luvuista $p_1, \dots, p_k$ olisi 3

$\Rightarrow 3 \nmid N = 4p_1 \cdots p_k + 3$.

Siis $q_i \neq 3$, jotenkin on löydetty uusi alkuluku muotoa $4n+3 \neq 3$.

Siis muotoa $4n+3$ olevien alkul. jonkko ei ole ääretön □

4 Ratkaistuja ja ratkaisemattomia kysymyksiä alkuluvuista

E. Landaun (1912) 4 tasmällisesti muotoiltua ongelmaa, joita L. piti sellaisina, joita tuolloin ei voida ratkaista. Ne ovat edelleen ratkaisemattomia.

4.1. Alkulukujen välejstä.

Koska alkulukujen tiheys välillä $[1,x]$ lähestyy 0:aa, kun $x \to \infty$, täytyy aina joskus olla monta yhdistettyä lukua.

Lause 4.1 Kaikille $n \geq 2$ on $n-1$ peräkkäistä yhdistettyä lukua.

Tod.

$2 \mid n! + 2$
$3 \mid n! + 3$
$\vdots$
$n-1 \mid n! + n-1$
$n \mid n! + n$

} koska $2 \mid n!$ ja $2 \mid 2$, peräkkäisiä yhd. lukuja ja $\square$

3 peräkkäistä yhd. luku a:

$$4! + 2 = 26$$
$$+3 = 27$$
$$+4 = 28$$

Eratosthenes: 8, 9, 10 ovat 3 peräkkäistä yhd. luku a.

Millaisia välejä alkuluvuille on?
2 ja 3 ovat ainoat peräkkäiset alkuluvut.
Entä alkuluvut, joiden erotus on 2?

Alkulukukaksoset

(3,5) (5,7) (11,13), (17,19), (29,31)

Avoin: Onko alkulukukaksosia ∞ monta?

Landau

Suurin alkulukukaksonen loyd. 2016 $2996863034895 \cdot 2^{1290000} \pm 1$

Euklid. lemma 1) p alkuluku, $a, b \in \mathbb{Z}$.

Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

2) Jos $p \mid a_1 \cdots a_n$, niin $p \mid a_1$ tai $p \mid a_2$ tai ... ... tai $p \mid a_n$

Esim. Jos $a, b, c \in \mathbb{Z}$ ja $p \mid abc$, niin $p \mid a$ tai $p \mid b$ tai $p \mid c$.

Jos p ei alkuluku voisi käydä näin: $4 \mid 2 \cdot 2$

mutta $4 \nmid 2$.

$3 \mid 9 \cdot 7 \cdot 15$ $\quad 3 \mid 9$, $3 \nmid 7$ $\quad 3 \mid 15$