Alkuluvuista sekä Fermat'n pieni lause

Palataan alkulukujen tarkasteluun.

Mersennen alkuluvut:
Muotoa $2^p - 1$ olevaa alkulukua sanotaan Mersennen alkuluvuksi. Muista ehdon suunta: Jos $2^p - 1$ on alkuluku, niin p on alkuluku. Toisinpäin ei päde, esim. $p = 11$ on alkuluku , mutta

$$2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89.$$

Fermat'n luvut:
Muotoa $2^m + 1$ olevaa alkulukua sanotaan Fermat'n luvuksi, merkitään F_n. Kuten Mersennen luvuissa, jos Fermat'n luku $2^m + 1$ on alkuluku, niin $m = 2^n$.
Tiedetään, että luvuista F_n alkulukuja ovat viisi ensimmäistä:

$$F_0 = 2^{2^0} + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 5, \qquad F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257, \qquad F_4 = 2^{2^4} + 1 = 65\,537$$

Euler osoitti, etteivät kaikki Fermat'n luvut ole alkulukuja, itseasiassa luku F_5 on yhdistetty luku. Ja tällä hetkellä yhtään lukua $F_n, n \geq 5$ ei tiedetä alkuluvuksi, muttei ole myöskään osoitettu etteikö jollakin n luku F_n olisi alkuluku.

Määritelmä, alkulukukaksoset ja alkulukuserkukset:
Jos p ja $p + 2$ ovat alkulukuja, niin paria $p, p + 2$ sanotaan *alkulukukaksosiksi*. Jos p ja $p + 4$ ovat alkulukuja, niin paria $p, p + 4$ sanotaan *alkulukuserkuksiksi.*
Esimerkiksi parit $(3, 5), (5\ 7), (11, 13), (17, 19)$ ja $(29, 31)$ ovat alkulukupareja. Suurin löydetty alkulukupari tällä hetkellä (2011 joulukuu) on

$$3756801695685 \cdot 2^{666669} \pm 1,$$

jossa on 200700 numeroa (http://primes.utm.edu/largest.html).

Määritelmä, alkulukujen määräfunktio (prime counting function):
Määritellään funktio $\pi\colon [0, \infty) \to \mathbb{N} \cup \{0\}$,

$$\pi(x) = \#\{p : p \text{ on alkuluku}, p \leq x\}, \qquad \text{missä } \# \text{ tarkoittaa lkm:ää.}$$

Siis annetulle luvulle x funktion π arvo $\pi(x)$ kertoo välillä $[0,x]$ olevien alkulukujen lukumäärän. Esimerkiksi

$$\pi(1)=0, \quad \pi(2)=1, \quad \pi(3)=2, \quad \pi(4)=2$$
$$\pi(5)=3, \quad \pi(6)=3, \quad \pi(7)=4, \quad \pi(7{,}5)=4$$
$$\pi(8)=4, \quad \pi(9)=4, \quad \pi(10)=4, \quad \pi(11)=5, \quad \text{jne.}$$

Jos alkulukujen määrä, eli arvo $\pi(x)$, välillä $[0,x]$ jaetaan välin pituudella x, niin saadaan alkulukujen esiintymistiheys $\frac{\pi(x)}{x}$ tällä välillä.

Esimerkki

x	2	7	25	100	500	5000
$\pi(x)$	1	4	9	25	95	669
$\frac{\pi(x)}{x}$	0,5	~0,57	0,36	0,25	0,19	~0,13

Huomaa, että $\frac{\pi(101)}{101}=\frac{26}{101}\approx 0{,}257 > \frac{\pi(100)}{100}=\frac{25}{100}=0{,}25$ eli funktio $\pi(x)$ ei ole vähenevä kaikkialla, mutta suuressa mittakaavassa on.

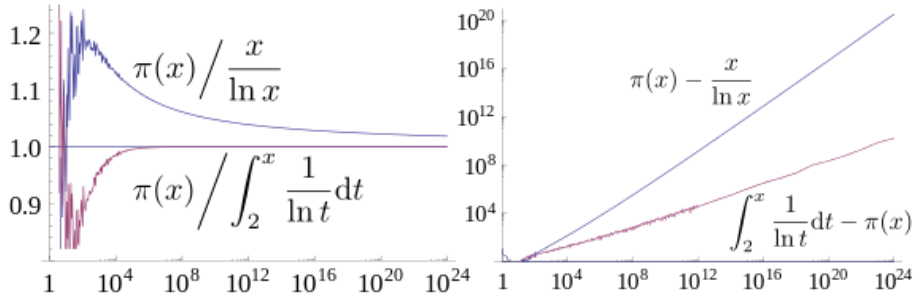
Koska alkulukuja on äärettömän paljon, niin $\pi(x)\to\infty$, kun $x\to\infty$.

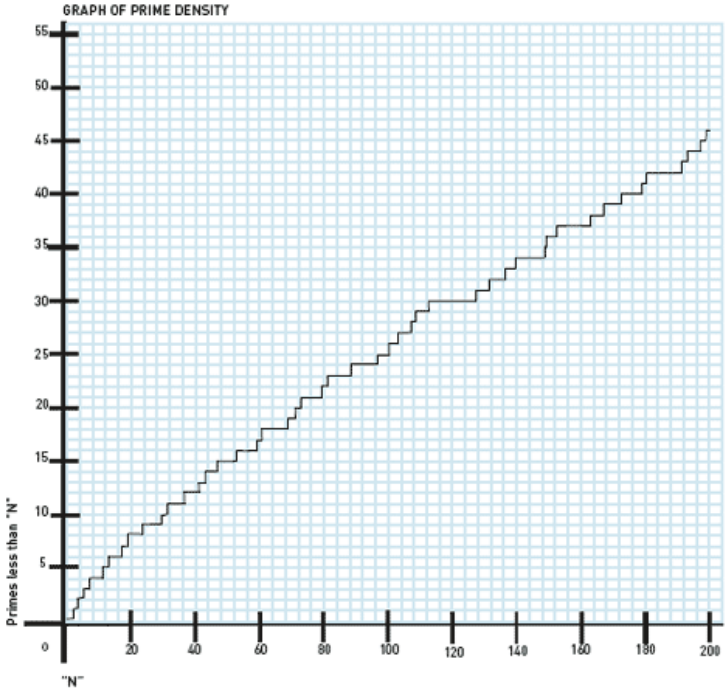
Alkulukujen esiintymistiheys $\frac{\pi(x)}{x}$ lähestyy kuitenkin nollaa, kun x lähestyy ääretöntä. Seuraava lause kertoo, että tiheyden lasku on hidasta; $\frac{\pi(x)}{x}$ lähestyy nollaa yhtä hitaasti kuin $\frac{1}{\ln x}$.

Lause, alkulukulause (prime number theorem):

$$\lim_{x\to\infty}\frac{\frac{\pi(x)}{x}}{\frac{1}{\ln x}}=\lim_{x\to\infty}\frac{\pi(x)}{x}\cdot\ln x=1.$$

Todistus: Todellinen harjoitustehtävä (vaikea)





Määritelmä, täydelliset luvut:
Sellaista luonnollista lukua, jonka kaikkien, luvusta itsestään poikkeavien tekijöiden summa on luku itse, sanotaan *täydelliseksi luvuksi*.

Esimerkki: Luvut $6 = 1 + 2 + 3$, $28 = 14 + 7 + 4 + 2 + 1$ ja luku $496 = 248 + 124 + 62 + 31 + 16 + 8 + 4 + 2 + 1$.

Tällä hetkellä (2013) tunnetaan 48 täydellistä lukua, joista kaikki ovat parillisia, yhtään paritonta täydellistä lukua ei tunneta.
(http://en.wikipedia.org/wiki/List_of_perfect_numbers)

Goldbach'in otaksuma eli konjektuuri:
Jokainen kahta suurempi parillinen luku on kahden alkuluvun summa.

Huom. Tiedetään, että konjektuuri on totta luvuille $> e^{e^{11503}}$, uskotaan…(http://mathworld.wolfram.com/GoldbachConjecture.html)

Lause, Fermat'n pieni lause (tärkeä):
Olkoon p alkuluku ja $a \in \mathbb{Z}$. Tällöin $[a^p]_p = [a]_p$. Ja jos oletetaan lisäksi, että $p \nmid a$, niin pätee myös

$$[a^{p-1}]_p = [1]_p.$$

Tämä on kirjan esittämä tapaus, siis sama asia kuin kongruenssi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Todistus: Keskellä on erittäin tärkeä havainto…missä luvut $c_1, c_2, c_3, \dots, c_{p-1}$ ovat luvut $1,2,3, \dots, p-1$ jossakin järjestyksessä.

Esimerkki Osoita, että $5^{152} \equiv 3 \pmod{11}$. Kirjoitetaan eksponentti toisin, jolloin

$$5^{152} = 5^{150+2} = 5^{150} \cdot 5^2 \equiv 5^{10 \cdot 15} \cdot 3 \pmod{11}$$

($25 = 11 \cdot 2 + 3$)

Koska $11 \in \mathbb{P}$ ja $\text{syt}(5,11) = 1$, niin Fermat'n pienen lauseen nojalla $5^{11-1} = 5^{10} \equiv 1 \pmod{11}$, josta edelleen saadaan

$$5^{10 \cdot 15} \cdot 3 \overset{\text{Fermat}}{\equiv} (1)^{15} \cdot 3 = 3 \pmod{11}, \qquad \text{OK.}$$