Lukuteoria 1 3.2.2022

4.1. Alkulukujen väleissä olevista raoista.

L.4.1 $\forall n \in \mathbb{N}-\{0\}$ on $n-1$ peräkkäistä yhdistettyä lukua.

$(\ n!+2, \ldots, n!+n\ )$

Määr. Jos p ja $p+2$ ovat alkulukuja, niin ne ovat alkulukukaksoset (twin primes)

Alkulukukaksoskonjektuuri: Alkulukukaksosia on ääretön määrä. (Auvin!)
(Landau)

suurin alkulukukaksospari.

(3,5) (5,7) (11,13) (17,19) (29,31) .... $(K \cdot 2^{1290000} \pm 1)$ v. 2016

Legendren konjektuuri (Landau) Lukujen n^2 ja $(n+1)^2$ välissä on alkuluku $\forall n \in \mathbb{N}-\{0\}$. (Avoin!)

1 4 9 16 25 36 ... (2,3) (5,7) (11,13) (17,19) (29)

4.2 Goldbachin konjektuuri (Landau)

Jokainen parillinen kokonaisluku ≥ 4 on kahden alkuluvun summa. (Avoin!)

$4 = 2+2$ $\quad 6 = 3+3$ $\quad 8 = 3+5$ $\quad 10 = 3+7$ $\quad 12 = 5+7$ $\quad 14 = 7+7$ $\quad 16 = 5+11$, $3+13$

$\Rightarrow$ $\forall$ parilliset $< 4 \cdot 10^{18}$ ovat 2 alkuluvun summia.

Helfgott (2022): Heikko Goldbachin konjektuuri: $\forall$ parittomat $n \geq 7$ ovat 3 alkuluvun summia.

4.3 Fermat'n luvut

$F_n = 2^{2^n} + 1$ on n:s Fermat'n luku.

$F_0 = 2^{2^0} + 1 = 3$

$F_1 = 2^2 + 1 = 5$

$F_2 = 2^4 + 1 = 17$

$F_3 = 2^8 + 1 = 257$

$F_4 = 2^{16} + 1 = 65537$

alkulukuja.

Fermat (1640): F_n on alkuluku $\forall n \in \mathbb{N}$.

Euler (1732): $F_5 = 641 \cdot 6700417$

Myöh. os. F_n on yhd. luku $\forall \; 5 \leq n \leq 32$

Ei ole löydetty sellaista $n \geq 5$, jolle F_n on alkuluku.

Uskotaan, että F_n on alkuluku $\Leftrightarrow$ $0 \leq n \leq 4$. (Avoin!)

$\Rightarrow$ (n^2+1)-konjektuuri (Landau): Muotoa n^2+1 olevia alkulukuja on ∞ monta. (Avoin!)

$1^2+1 = 2$ $\quad 2^2+1 = 5$ $\quad 3^2+1 = 10$ $\quad 4^2+1 = 17$ $\quad 5^2+1 = 26$ $\quad 6^2+1 = 37$ ...

Iwaniec (1978) on ääretön monta lukua n^2+1, jotka ovat alkulukuja tai 2 alkuluvun tuloja.

4.4. Mersennen luvut

p alkuluku $M_p = 2^p - 1$ Mersennen luku

Jos M_p on alkuluku, niin se on Mersennen alkuluku.

$M_2 = 2^2 - 1 = 3$
$M_3 = 2^3 - 1 = 7$
$M_5 = 2^5 - 1 = 31$
$M_7 = 2^7 - 1 = 127$
} alkul.

$M_{11} = 2047 = 23 \cdot 89$

Avoin kysymys: Onko Mersennen alkulukuja ∞ monta?

Tunnetaan 51 Mersennen alkulukua.
$\forall$ eksponentit $\leq 107 \cdot 10^6$ laskettu ainakin kerran

Suurin tunnettu alkuluku on Mersennen luku. (2018)

5 Kongruenssi

Määr. Olk. $m \in \mathbb{N}-\{0,1\}$. Luvut $a,b \in \mathbb{Z}$ ovat kongruentteja $\left\{\begin{array}{l}\text{modulo } m\\ \text{mod } m\\ \text{luvun } m \text{ suhteen}\end{array}\right.$

jos $m \mid (a-b)$. Tällöin merk. $a \equiv b \bmod m$.

$\Updownarrow$

$a-b = km \Leftrightarrow a = b+km$ jollain $k \in \mathbb{Z}$.

Esim. (1) $m=5$: $1 \equiv 6 \bmod 5$ $\quad 2 \equiv 12 \bmod 5$ jne.

(2) $n \in \mathbb{Z}$ on parillinen $\Leftrightarrow \exists\, k \in \mathbb{Z} : (n = 2k \Leftrightarrow n-0 = 2k)$

$\Leftrightarrow n \equiv 0 \bmod 2$.

(3) $m \mid n \Leftrightarrow n \equiv 0 \bmod m$.

Lemma (1) $a \equiv a \mod m \quad \forall\, a \in \mathbb{Z}$

(2) $a \equiv b \mod m \iff b \equiv a \mod m$

(3) $a \equiv b \mod m$ ja $b \equiv c \mod m \Rightarrow a \equiv c \mod m.$

$x \equiv y \mod m \iff m \mid x-y$

Tod. (1) $a - a = 0$ ja $m \mid 0$ (L. 1.3)

(2) $a \equiv b \mod m \iff m \mid (a-b) \iff m \mid (b-a) \iff b \equiv a \mod m.$

$b - a = -(a-b)$

(3) $a \equiv b \mod m \iff m \mid a-b$

$b \equiv c \mod m \iff m \mid b-c$ } L.1.3 $\Rightarrow m \mid \underbrace{(a-b)+(b-c)}_{a-c} \iff a \equiv c \mod m.$ □

Lemma 1) Jos $a \equiv b \mod n$ } niin $a \equiv b \mod d$
$d \mid n$ }

2) Jos $a \equiv r \mod n$, niin $a = qn + r$
ja $0 \le r \le n-1$

(5) **Tod.** 1) $a \equiv b \mod n \iff n \mid (a-b)$ } L.1.3 $\Rightarrow$ $d \mid (a-b) \iff a \equiv b \mod d.$
$d \mid n$

Lause 5.4 Olk. $n \in \mathbb{N} - \{0,1\}$.

(1) Jos $a \equiv b \bmod n$, niin $ax + cy \equiv bx + dy \bmod n \quad \forall x, y \in \mathbb{Z}$.
$c \equiv d \bmod n$

(2) Jos $a \equiv b \bmod n$, niin $ac \equiv bd \bmod n$.
$c \equiv d \bmod n$

(3) Jos $a \equiv b \bmod n$, niin $a^m \equiv b^m \bmod n \quad \forall m \in \mathbb{N}$.

Esim. Mikä on luvun 3^{400} viimeinen numero 10-järjestelmässä?

Tark. kongruenssia mod 10. Viimeinen numero on $0 \le r \le 9 = 10 - 1$

s.e. $r \equiv 3^{400} \bmod 10$.

$10 \mid (3^{400} - r)$

Huom. $3^4 = 81 \equiv 1 \bmod 10$

$$3^{400} = (3^4)^{100} \underset{\text{L.5.4 (3)}}{\equiv} 1^{100} = 1 \Rightarrow \text{viimeinen numero on } 1.$$

L. 5.4 todistus. $n \mid (b-a)$, $n \mid (c-d)$

(1) $ax+cy \equiv bx+dy$

$ax+cy-(bx+dy) = (a-b)x + (c-d)y$

L. 1.3 : $n \mid (a-b)x + (c-d)y$. $\Rightarrow$ $ax+cy \equiv bx+dy \mod n$.

(2) $ac \equiv bd$

L. 1.3 : $n \mid \big((b-a)c + (d-c)b\big)$

$= bc - ac + bd - bc$

$\Rightarrow n \mid bd-ac$

$\Leftrightarrow ac \equiv bd \mod n$.

(3) (2) + induktio.