Lukuteoria 1 24.2.2022

Eulerin funktio $\varphi : \mathbb{N}-\{0\} \to \mathbb{N}-\{0\}$

$\mathcal{R}(n) = \{ 1 \leq k \leq n : \text{syt}(k,n) = 1 \}.$

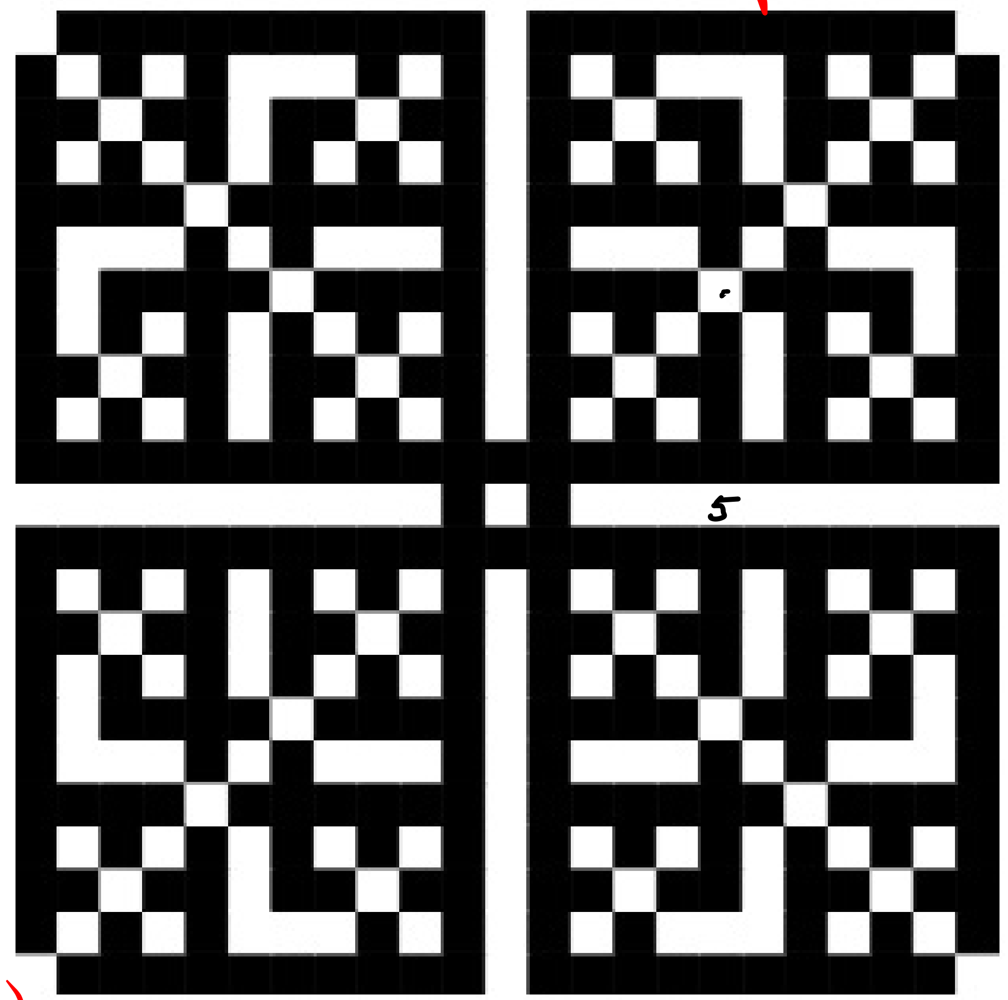
$\mathcal{R}(1) = \{1\}$, $\mathcal{R}(2) = \{1\}$

$\mathcal{R}(3) = \{1,2\}$ $\mathcal{R}(4) = \{1,3\}$

$\varphi(n) = \# \mathcal{R}(n).$

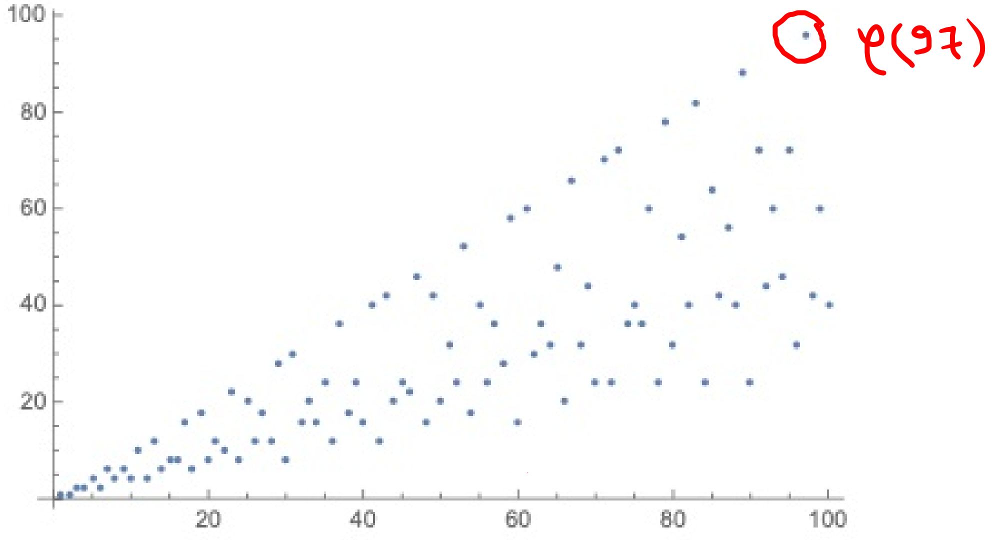
Jos n on alkuluku,
niin $\varphi(n) = n-1$

Suhteelliset alkulukuparit



■ kohdassa (m,n) : $\text{syt}(m,n) = 1$

□ $\neq 1$



Kuva 6.1 — Eulerin ϕ-funktion arvot $\phi(n)$, kun $1 \leqslant n \leqslant 100$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
$\phi(n)$	12	10	22	8	20	12	18	12	28	8	30	16	20	16	24	12	36	18	24	16

Määr. $f: \mathbb{N}-\{0\} \to \mathbb{Z}$ on multiplikatiivinen funktio, jos

$f(mn) = f(m)f(n)$ kaikille m, n, joille $\mathrm{syt}(m,n) = 1$.

Esim $\varphi(20) = 8 = 2 \cdot 4 = \varphi(4)\varphi(5)$ $\quad (20 = 4 \cdot 5,\ \mathrm{syt}(4,5) = 1)$

Lause 6.11 φ on multiplikatiivinen funktio.

Lemma 6.12 Jos p on alkuluku, niin $\varphi(p^k) = p^{k-1}(p-1)$

Tod. Harjoitustehtävä.

Esim. $60 = 3\cdot 20 = 2^2\cdot 3\cdot 5$

L.6.11, L.6.12: $\underline{\underline{\varphi(60)}} = \varphi(2^2\cdot 3\cdot 5) = \varphi(2^2)\,\varphi(3\cdot 5) = \varphi(2^2)\,\underset{=2}{\varphi(3)}\,\underset{=4}{\varphi(5)}$

$\overset{\text{L.6.12}}{=} 2\cdot(2-1)\cdot 2\cdot 4 = \underline{\underline{16}}$

$\left.\begin{array}{l}\varphi(59) = 58\\ \varphi(61) = 60\end{array}\right\}$ koska 59, 61 alkulukuja.

L.6.11 tod. Olk. $m_1, m_2 \in \mathbb{N}-\{0\}$, $\mathrm{syt}(m_1, m_2) = 1$.

$F: \overbrace{\mathcal{R}(m_1 m_2)}^{\# = \varphi(m_1 m_2)} \to \underbrace{\mathcal{R}(m_1)\times\mathcal{R}(m_2)}_{\# = \varphi(m_1)\varphi(m_2)}$

$F(x) = (r_1, r_2)$, missä $\begin{cases} r_1 \equiv x \mod m_1\\ r_2 \equiv x \mod m_2\end{cases}$

Väite seuraa, jos os. että F on bijektio.

Pitää tarkastaa, että $r_1 \in \mathcal{R}(m_1)$ ja $r_2 \in \mathcal{R}(m_2)$: Os. että $\mathrm{syt}(m_1, r_1) = 1 = \mathrm{syt}(m_2, r_2)$: $\mathrm{syt}(x, m_1) = 1$, koska x:n ja m_1:n yht. tekijä on x:n ja $m_1 m_2$:n yht. tekijä.

Jakojäännös, kun x jaetaan m_1:llä: $x = a m_1 + r_1$, $0 \le r_1 \le m_1 - 1$

Jos $d \mid x$ ja $d \mid m_1$ $\Rightarrow$ $d \mid r_1 = x - a m_1$

Jos $d \mid r_1$ ja $d \mid m_1$ $\Rightarrow$ $d \mid x = r_1 + a m_1$

$\leadsto$ $1 = \text{syt}(x, m_1) = \text{syt}(r_1, m_1)$. Vast. nähd $\text{syt}(r_2, m_2) = 1$.

Siis F:n määrittely on OK.

Jakoyhtälö: Jokaisella x on 1-käs $0 \le r_2 \le m_2 - 1$, $0 \le r_1 \le m_1 - 1$ s.e.

$$(*) \begin{cases} r_1 \equiv x \mod m_1 \\ r_2 \equiv x \mod m_2 \end{cases}$$

Edellä nähtiin, että $r_1 \in \mathcal{R}(m_1)$, $r_2 \in \mathcal{R}(m_2)$

Kiinalainen jäännöslause: yhtälöparilla $(*)$ on 1-käs ratkaisu mod $m_1 m_2$

$\Rightarrow$ F on bijektio. $\square$

Fermat'n pieni lause (L. 5.22): Jos p on alkuluku ja $p \nmid a$, niin

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

Kaikille $a \in \mathbb{Z}$ pätee $a^p \equiv a \mod p$.

Lause 6.10 (Eulerin yleistys Fermat'n pienelle lauseelle) Olk.

$a, n \in \mathbb{N} - \{0\}$. Tällöin

$\operatorname{syt}(a, n) = 1$

$$a^{\varphi(n)} \equiv 1 \mod n$$

Tod. $\mathcal{R}(n) = \{b_1, \dots, b_{\varphi(n)}\}$.

$$a^{\varphi(n)} b_1 \cdots b_{\varphi(n)} = \underbrace{(a b_1)}_{\operatorname{syt}(a b_1, n) = 1} (a b_2) \cdots (a b_{\varphi(n)}) \equiv b_1 b_2 \cdots b_{\varphi(n)}$$

S. 5.8

$\Rightarrow a^{\varphi(n)} \equiv 1 \mod n.$ $\square$

$a b_1 \equiv a b_2 \mod n \Rightarrow b_1 \equiv b_2 \mod n$

5

Esim. Luvun 3^{1000} viimeinen numero 10-järjestelmässä.

Lasketaan $3^{1000} \bmod 10$ edustaja/jakojäännös 10:llä jaettaessa.
$\in \{0, \dots, 9\}$.

$$\varphi(10) = \underbrace{\varphi(2)}_{1}\underbrace{\varphi(5)}_{4} = 4$$

L.6.10: $3^4 = 3^{\varphi(10)} \equiv 1 \mod 10$ (Huom syt$(3,10)=1$)

$$3^{1000} = 3^{\varphi(10)\cdot 250} \equiv 1^{250} = 1$$

Siis viimeinen numero on 1.

Harj. Luvun 3^{400} 2 viimeistä numeroa.

Lause 6.13 $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_N}\right)$

$$n = p_1^{e_1} p_2^{e_2} \cdots p_N^{e_N}$$

Tod. $n = p_1^{e_1} \cdots p_N^{e_N}$ eri alkuluvut ovat sulut. alkulukuja

$$\varphi(n) \underset{L.6.11}{=} \varphi(p_1^{e_1}) \cdots \varphi(p_N^{e_N}) \underset{L.6.12}{=} p_1^{e_1-1}(p_1-1)\, p_2^{e_2-1}(p_2-1) \cdots p_N^{e_N-1}(p_N-1)$$

$$= p_1^{e_1}\left(1-\frac{1}{p_1}\right) \cdots p_N^{e_N}\left(1-\frac{1}{p_N}\right) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_N}\right).$$

$\square$

Esim. $175 = 7 \cdot 25 = 5^2 \cdot 7$

$$\varphi(175) = \underbrace{175}_{5^{\cancel{2}} \cdot \cancel{7}} \underbrace{\left(1-\frac{1}{5}\right)}_{\frac{4}{\cancel{5}}} \underbrace{\left(1-\frac{1}{7}\right)}_{\frac{6}{\cancel{7}}} = 4 \cdot 5 \cdot 6 = 120.$$