Arvuteooria vanemale rühemale

Vahur Paist

Detsember 2024

1 Põhitõed

• Täisarvude a ning b korral kirjutame $a \mid b$ kui leidub täisarv c, nii et $a \cdot c = b$. Kõnekeeles öeldakse, et a **jagab** b-d.

• Täisarvud a ning b on **kongruentsed mooduli** n **järgi** parajasti siis kui vahe $a - b$ jagub arvuga n, ehk

$$n \mid a - b \iff a \equiv b \pmod{n}$$

2 Euleri teoreem ning Fermat' väike teoreem

Teoreem 1 (Euleri teoreem). Olgu n positiivne täisarv ning a temaga ühistegurita positiivne täisarv. Siis

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Siinkohas märgime tähisega $\phi(n)$ positiivsete täisarvude arvu, mis on väiksemad kui n ning ühistegurita arvuga n.

Järeldus 1 (Fermat' väike teoreem). Olgu p algarv täisarv ning a temaga ühistegurita positiivne täisarv. Siis

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

Teoreem 2 (Wilsoni teoreem) Konguents

$$(n-1)! \equiv -1 \pmod{n}$$

kehtib parajasti siis kui n on algarv.

3 Ülesanded

Ülesanne 1. Tõesta, et kui n ei jagu arvuga 17, siis üks arvudest n^8+1, n^8-1 jagub.

Ülesanne 2. Leia arvu 7^{2042} viimased kaks numbrit

Ülesanne 3. Näita et, $n \mid 2^{n!}-1$ iga paaritu positiivse n korral

Ülesanne 4. Tõesta, et iga täisarvu k korral leidub k järjestikust täisarvu, mis ei ole algarvud ega algarvu astmed.

Ülesanne 5. (MONT lk 56) Näita, et jääk mis tekkib $(p-1)!$ jagamisel $p(p-1)$-ga on $p-1$

Ülesanne 6. (BT 2018-18) Olgu $n \geqslant 3$ selline täisarv, et arv $4n+1$ on algarv. Tõesta, et $4n+1 \mid n^{2n}-1$

Ülesanne 7. Olgu $p = 2q+1$ paaritu algarv. Tõesta, et p jagab arvu $(q!)^2 + (-1)^q$

Ülesanne 8. (IMO 2005) Leia kõik positiivsed täisarvud, mis on ühistegurita kõigi jada $(a_n)_{n=1}^{\infty}$

$$a_n = 2^n + 3^n + 6^n - 1$$

liikmetega.

Ülesanne 9. (ARML 2002) Olgu a postiivne täisarv, nii et

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{23} = \frac{a}{23!}$$

Leia jääk mis tekkib a jagamisel 13-ga.

Ülesanne 10. Tõesta, et iga algarvu p ning täisarvu k korral $0 \leqslant k \leqslant p-1$:

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

Ülesanne 11. (USAMO 1991) Näita, et iga täisarvu $n \geqslant 1$, korral on kõik jada liikmed

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, ...$$

mingist liikmest alates kongruentsed *modulo* n