Lukuteoria 1 15.2.2022

Luku $c \in \mathbb{Z}$ on lukujen $a_1, a_2, \ldots, a_N \in \mathbb{Z} - \{0\}$ *yhteinen jaettava*, jos $a_i \mid c$ kaikilla $1 \leqslant i \leqslant N$. Lukujen $a_1, a_2, \ldots, a_N \in \mathbb{Z} - \{0\}$ *pienin yhteinen jaettava*, $\operatorname{pyj}(a_1, a_2, \ldots, a_N)$ on niiden pienin positiivinen yhteinen jaettava.

$|a_1 a_2 \cdots a_N| > 0$ on yhteinen jaettava

Lause 2.20 $a \mid c$ ja $b \mid c \iff \operatorname{pyj}(a,b) \mid c$

Lause 2.22 $\operatorname{syt}(a,b)\operatorname{pyj}(a,b) = ab$.

Tod. Käytä yl. alkutekijäesitystä.

Lause 5.10 $m_1, \ldots, m_r \in \mathbb{N} - \{0,1\}$, $x, y \in \mathbb{Z}$.

Tällöin $x \equiv y \bmod m_k \ \forall\, 1 \leq k \leq r \iff x \equiv y \bmod \operatorname{pyj}(m_1, \ldots, m_r)$.

Seuraus Jos $p_1, \ldots, p_r$ on alkulukuja, $x, y \in \mathbb{Z}$.

Tällöin $x \equiv y \bmod p_k \ \forall\, 1 \leq k \leq r \iff x \equiv y \bmod p_1 p_2 \cdots p_r$.

① $\left(\operatorname{pyj}(p_1, \ldots, p_r) = p_1 p_2 \cdots p_r$ 2.2.22 nojalla, sillä $\operatorname{syt}(p_1, \ldots, p_r) = 1\right)$

L. 5.10:n tod. Jos $x \equiv y \bmod m_i \underset{\text{määr}}{\iff} m_i \mid x-y$, niin $x-y$ on luvuista

$m_1, \dots, m_r$ yhteinen jaettava.

L. 2.20 $\Rightarrow$ $\operatorname{pyj}(m_1, \dots, m_r) \mid x-y \iff x \equiv y \bmod \operatorname{pyj}(m_1, \dots, m_r)$.

Jos $x \equiv y \bmod \operatorname{pyj}(m_1, \dots, m_r) \iff \begin{cases} \operatorname{pyj}(m_1, \dots, m_r) \mid x-y \\ m_k \mid \operatorname{pyj}(m_1, \dots, m_r) \end{cases} \Rightarrow m_k \mid x-y$

$\Updownarrow$

$x \equiv y \bmod m_k$.

Viimeksi: Fermat'n pieni lause: Jos p on alkuluku, niin kaikille $a \in \mathbb{Z}$ pätee $a^p \equiv a \bmod p$.

Wilsonin lause Olk. $n \in \mathbb{N} - \{0,1\}$. Tällöin n alkuluku, jos ja vain jos $(n-1)! \equiv -1 \bmod n$.

Tod. Harj. 3.16: Jos $n \geq 5$ on yhd. luku, niin $(n-1)! \equiv 0 \bmod n$.

$n = 4$; $(n-1)! = 3! = 6$ ei ole jaollinen 4:llä.

Ol. etta p on alkuluku.

Lemma 5.20: Jos $p \nmid a$, niin on b s.e. $ab \equiv 1 \bmod p$.

Tod. **Bézout:** Koska syt$(a,p) = 1$, on $x, y \in \mathbb{Z}$:

$$ax + py = 1 \Rightarrow ax \equiv 1 \bmod p$$
$$\Leftrightarrow ax - 1 = py$$

(Idea: $(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (p-1)$
$= \quad = \quad \equiv$
L. 5.20 $\equiv 1 \quad -1 \bmod 7$

$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = (2 \cdot 4)(3 \cdot 5)\,6 \equiv 1 \cdot 1 \cdot (-1) = -1 \bmod 7$
$= \quad \equiv \quad = \quad \equiv$

$2 \cdot 4 \equiv 1 \bmod 7$
$3 \cdot 5 = 15 \equiv 1 \bmod 7$

Etsitään luvulle $2 \leq a \leq p-2$ pari $b \neq a$, $2 \leq b \leq p-2$
s.e. $ab \equiv 1 \bmod p$. Tulosta $(p-1)!$ (oā vain $p-1 \equiv -1 \bmod p$)

Luvun a pari b löytyy aina seur. lemman perusteella:

Lemma. Yhtälöllä $x^2 \equiv 1 \bmod p$ on tasmalleen 2 ratkaisua $x = 1$ ja $x = p-1$ välillä $1 \le x \le p-1$.

Lemman tod. $1^2 = 1 \equiv 1 \bmod p$.

$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \bmod p$.

} 1 ja $p-1$ ovat ratkaisuja.

Jos $x^2 \equiv 1 \bmod p$, niin $p \mid x^2 - 1 = \underbrace{(x+1)}_{\in \mathbb{Z}} \underbrace{(x-1)}_{\in \mathbb{Z}}$

↑ alkuluku

Eukl. lemma

$\Rightarrow p \mid x+1 \iff x \equiv -1 \bmod p$ Jos $1 \le x \le p-1$, niin $x = p-1$

tai $p \mid x-1 \iff x \equiv 1 \bmod p$ —"— $x = 1$. □

Yhtälöllä $ab \equiv 1 \bmod p$ on 1-käs. ratkaisu $2 \le b \le p-2$, kun $2 \le a \le p-2$:

Jos $ab_1 \equiv 1 \equiv ab_2 \bmod p$, niin $b_1 \equiv b_2 \bmod p$ s. s. 8 nojalla ($\mathrm{syt}(a,p) = 1$)

Siis $(p-1)! = 1 \cdot \underbrace{2}_{a} \cdots \underbrace{(p-2)}_{b}(p-1) \equiv 1 \cdot \underbrace{1 \cdots 1}_{\frac{p-3}{2}} \cdot (-1) = -1 \mod p.$ □

$ab \equiv 1 \mod p$

Polynomit ja kongruenssi

Lause 5.27 Olk. $P(x) = \underbrace{c_0}_{\in \mathbb{Z}} + \underbrace{c_1}_{\in \mathbb{Z}} x + \cdots + \underbrace{c_k}_{\in \mathbb{Z}} x^k$ kokonaislukukertoiminen polynomi

Jos $a, b \in \mathbb{Z}$, $a \equiv b \mod n$, niin $P(a) \equiv P(b) \mod n$.

Tod. **L. 5.4:** $a^j \equiv b^j \mod n \quad \forall \; 1 \le j \le k.$

$\Rightarrow c_j a^j \equiv c_j b^j \mod n$

5.5 $\underbrace{c_0 + c_1 a + c_2 a^2 + \cdots + c_k a^k}_{P(a)} \equiv \underbrace{c_0 + c_1 b + \cdots + c_k b^k}_{P(b)} \mod n$ □

Määr. Luku $a \in \mathbb{Z}$ on kokonaislukukertoimisen polynomin $P(X)$ **juuri**, jos $P(a) = 0$.

Seuraus 5.28 Jos on $n \in \mathbb{N}$ s.e. yhtälöllä $P(X) \equiv 0 \bmod n$ ei ole ratkaisua, niin { polynomilla $P(X)$ ei ole juurta. / polynomiyhtälöllä $P(X) = 0$ ei ole ratkaisua kokonaislukujen joukossa.

Tod. Jos $P(X) = 0$, niin $P(X) \equiv 0 \bmod n$.

Jos $P(x) \not\equiv 0$ kaikilla x, niin $P(x)$ ei voi olla 0. $\Rightarrow \leftarrow$

Esim. Os. että polynomilla $P(x) = x^7 - x + 1$ ei ole juurta.

Tarkastellaan kysymystä mod 2: Jos $x \equiv 0 \bmod 2$, niin

$P(x) \equiv 0^7 - 0 + 1 = 1 \not\equiv 0 \bmod 2$.

Jos $x \equiv 1 \bmod 2$, niin $P(x) \equiv 1^7 - 1 + 1 = 1 \not\equiv 0 \bmod 2$.

Kongr. luokkia mod 2 on 2 kpl, molemmat tarkastettu. Seuraus 5.28 $\Rightarrow P(x) \neq 0 \ \forall x \in \mathbb{Z}$.

$Q(x) = x^7 - x + 2$.

mod 2: Jos $x \equiv 0 \bmod 2$, niin $Q(x) \equiv 0^7 - 0 + 2 \equiv 0 \bmod 2$

Kongruenssiluokka $Q(x) \equiv 0 \bmod 2$ on ratkaisu.

mod 3: Jos $x \equiv 0 \bmod 3$, niin $Q(x) \equiv 0^7 - 0 + 2 \not\equiv 0 \bmod 3$.

Jos $x \equiv 1 \bmod 3$, niin $Q(x) \equiv 1^7 - 1 + 2 = 2 \not\equiv 0 \bmod 3$

Jos $x \equiv 2 \bmod 3$, niin $x \equiv -1 \bmod 3$. Tällöin

$Q(x) \equiv (-1)^7 - (-1) + 2 = -1 + 1 + 2 = 2 \not\equiv 0 \bmod 3$

kokonaisluvuilla.

S. 5. 28 $\Rightarrow$ Polynomilla $Q(x)$ ei ole juuria.

Esim. Ei ole kokonaisluvuilla polynomia $P(x)$, jolla aste ≥ 1, jolle $P(k)$ on alkuluku $\forall k \in \mathbb{Z}$. Jos $P(x)$ olisi tällainen polynomi, niin $P(k_0)$ olisi alkuluku jollain $k_0 \in \mathbb{Z}$. Tark. mod $P(k_0) \in \mathbb{N} - \{0, 1\}$

L. 5. 27: $\underbrace{P(b)}_{\text{alkuluku}} \equiv \underbrace{P(k_0)}_{\equiv 0} \bmod P(k_0)$ $\forall\, b \equiv k_0 \bmod P(k_0)$.

$\Rightarrow P(k_0) \mid P(b) \Rightarrow P(b) = P(k_0)$

$\Rightarrow$ Polynomille $Q(x) = P(x) - P(k_0)$ pätee

$$Q(b) = P(b) - P(k_0) = 0 \quad \forall\ b \equiv k_0 \bmod P(k_0).$$

Tällaisia b on ääretön monta.

Polynomifunktiolla Q on ääretön monta 0-kohtaa ellei $Q(x)=0$-poly.

$\Rightarrow P(x) = P(k_0)$ on vakiopolynomi.