

Algebra
Syksy 2009
Harjoitus 4 (vko 40)

- a) Olkoot $a, b \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Osoita, että $(n - a)^2 \equiv a^2 \pmod{n}$,

b) Osoita, että jos p on alkuluku, niin $\text{syty}((p-1)!, p) = 1$.
- Mitä on $5^{2000000} \pmod{24}$?
- Määrää Fermat'n pienen lauseen avulla pienin ei-negatiivinen jäännös, kun
 - 3^{1000} jaetaan luvulla 7,
 - 2^n jaetaan luvulla 17, missä $16 \mid n$.
- Jos $k \equiv 1 \pmod{4}$, niin minkä luvuista 0, 1, 2, 3 kanssa kongruentti modulo 4 on luku
 - $6k + 5$?
 - $2k^3 + k + 3$?
- Onko kokonaislukujen **a)** kertolasku, **b)** yhteenlasku, laskutoimitus joukossa $A = \{1, -1, 0\}$? Perustelee!
- Mitkä seuraavista operaatioista/säännöistä **eivät** ole laskutoimituksia eli binäärioperaatioita? Miksi?
 - Parittomien kokonaislukujen joukossa: lukupariin liitetään niiden keskiarvo.
 - Rationaalilukujen joukossa: lasketaan kolmen luvun tulo.
 - Reaalilukujen joukossa: $a * b := (a + 2b)/a$.
 - Luonnollisten lukujen joukossa: $n * m := 5$.
- Ovatko kokonaislukujoukon \mathbb{Z} laskutoimitukset \circ
 - $x \circ y = x$,
 - $x \circ y = |x - y|$,
 - $x \circ y = x + y - 1$,liittännäisiä ja/tai vaihdannaisia?